Access Operating System (AOS) Command Reference

Release 5.0
Part Numbers 220-0173-01, 220-0174-01, 220-0175-01
Order Number TPCR-5.0

Corporate Headquarters
Redback Networks Inc.
250 Holger Way
San Jose, CA 95134-1362
USA
http://www.redback.com
Tel: 408-571-5000

© 1998–2001, Redback Networks Inc. All rights reserved.

Redback is a U.S. registered trademark of Redback Networks Inc. NetOp, Network Services Contractor, NSC, SmartEdge, SMS, VEM, Virtual Enterprise Manager, and “Building the New Access Network” are trademarks of Redback Networks Inc. SSH is a Registered Trademark of SSH Communications Security Ltd. All other marks are the property of their respective owners.

Rights and Restrictions

All statements, specifications, recommendations, and technical information contained are current or planned as of the date of publication of this document. They are reliable as of the time of this writing and are presented without warranty of any kind, expressed or implied. In an effort to continuously improve the product and add features, Redback Networks Inc. (“Redback”) reserves the right to change any specifications contained in this document without prior notice of any kind.

Redback shall not be liable for technical or editorial errors or omissions which may occur in this document. Redback shall not be liable for any indirect, special, incidental or consequential damages resulting from the furnishing, performance, or use of this document.

Limited Hardware Warranty and Disclaimer

Limited Warranty. Redback warrants to the original purchaser of the product (“Purchaser”) only that the hardware sold hereunder shall be free of defects in material and workmanship and shall perform, under normal use and circumstances, in accordance with Redback's published specifications for a period of ninety (90) days from the shipment date. In the event that Redback receives notice from Purchaser during the warranty period that any hardware does not conform to its warranty, Redback shall, at its sole option (and as Purchaser’s sole remedy), either repair or replace the non-conforming hardware, or refund the purchase price of such unit. Hardware replaced under the terms of any such warranty may be refurbished or new equipment substituted at Redback's option. This warranty is the only warranty made by Redback with respect to the hardware delivered hereunder and may be modified, amended or supplemented only by a written instrument signed by a duly authorized officer of Redback and accepted by Purchaser.

Procedures. A hardware item may only be returned with the prior written approval of Redback. Any such approval shall reference a return material authorization number issued by authorized Redback service personnel. Transportation costs, if any, incurred in connection with the return of a defective item to Redback shall be borne by Purchaser. Any transportation costs incurred in connection with the re-delivery of a repaired or replaced item to Purchaser shall be borne by Redback; provided that, such costs shall be borne by Purchaser if Redback reasonably determines that the item is not defective. If Redback determines, in its sole discretion, that the allegedly defective item is not covered by the terms of the warranty provided hereunder or that a warranty claim is made after the warranty period, the cost of repair by Redback, including all shipping expenses, shall be reimbursed by Purchaser.

Exclusions. The foregoing warranties and remedies are for Purchaser's exclusive benefit and are non-transferable. The foregoing warranties do not apply to any hardware which (1) has been altered, except as authorized by Redback, (2) has not been installed, operated, repaired, or maintained in accordance with any installation, handling, maintenance, or operating instructions supplied by Redback, (3) has been subjected to unusual physical or electrical stress, misuse, negligence, or accident (4) is used in ultrahazardous activities, (5) has been damaged or rendered unserviceable by installation or use outside of environmental specifications, or (6) has been exported from the original country of destination. In no event does Redback warrant that Purchaser will be able to operate its networks without problems or interruptions.

Third Party Products. Where a product not manufactured by Redback is sold by Redback hereunder to complete an order, the warranty coverage on that product is limited to its original manufacturer's warranty to the Purchaser, if any.

THE LIMITED WARRANTIES SET FORTH ABOVE ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY OR OTHERWISE, AND REDBACK SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. REDBACK DOES NOT WARRANT THAT THE PRODUCTS WILL MEET PURCHASER'S REQUIREMENTS OR THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE.

Software License Agreement

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. BY INSTALLING AND USING REDBACK SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT USE THE REDBACK SOFTWARE PRODUCTS.

Software. The software covered by this license agreement includes all Redback proprietary software, whether provided on magnetic media, loaded on the product or embedded in the product as firmware, and any third party software licensed to Redback included therein (jointly, the “Software”).

License. Subject to the terms and conditions of this Agreement, Redback grants to the original end user of the products (“Licensee”) a personal, nonexclusive and nontransferable license to use the specific Redback base program, supplement(s) or feature set(s) Software and related product documentation (the “Documentation”) for which Licensee has paid the required license fees, in object code form only, in accordance with the terms and conditions of this agreement solely in connection with the use of Redback equipment, on a single hardware chassis, or on a single central processing unit, as applicable, owned or leased by Licensee. If Licensee has purchased a multi-user license, then, subject to the terms and conditions of this Agreement, Licensee is granted a nonexclusive and nontransferable license to allow the number of simultaneous users authorized under such license and for which Licensee has paid the required license fee to use the Software.

Copies. Licensee agrees not to make any copies of the Software or the Documentation, in whole or in part, other than one copy for archival purposes only. Licensee agrees not to modify, translate, reverse engineer, de-compile, disassemble, or create derivative works based on the Software, except to the extent that the such limitation is prohibited by applicable law. Licensee agrees to take reasonable steps to safeguard copies of the Software against disclosure, copying or use by unauthorized persons, and to take reasonable steps to ensure that the provisions of this license are not violated by Licensee’s employees or agents.

Proprietary Information. Licensee agrees that aspects of the Software and Documentation constitute trade secrets and/or copyrighted material of Redback or its suppliers. Licensee shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material to any third party without the written consent of Redback.

Title. All right, title and interest in and to the Software and Documentation, including all intellectual property rights therein, shall remain the property of Redback or its suppliers, subject only to the limited license granted to Licensee. This license is not a sale and does not transfer to Licensee any title or ownership in or to the Software or the Documentation or any patent, copyright, trade secret, trade name, trademark or other proprietary or intellectual property rights related thereto.

Limited Warranty. Redback warrants to Licensee only that the media on which the Software is recorded shall be free from defects in materials and workmanship under normal use for a period of 90 days from the date of shipment by Redback. Licensee's exclusive remedy, and Redback's exclusive liability, shall be replacement of the media in accordance with this limited warranty. THE SOFTWARE IS PROVIDED "AS IS." REDBACK EXPRESSLY DISCLAIMS AND NEGATES ALL WARRANTIES FOR THE SOFTWARE, WHETHER EXPRESSED, IMPLIED, STATUTORY OR OTHERWISE, AND REDBACK SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF INTELLECTUAL PROPERTY OR OTHER VIOLATION OF RIGHTS. Redback does not warrant that the Software will meet Licensee's requirements or that the operation of the Software will be uninterrupted or error free. This warranty gives Licensee specific legal rights. Licensee may also have other rights, which vary from state to state or country to country.

Limitation of Liability. IN NO EVENT WILL REDBACK OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE EVEN IF REDBACK OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Redback or its suppliers' liability to Licensee, whether in contract, tort (including negligence), or otherwise, exceed the license fees paid by Licensee. Some states or countries do not allow exclusion or limitation of incidental or consequential damages or limitation on how long an implied warranty lasts, so the above limitations or exclusions may not apply to Licensee.

Termination. This agreement shall continue in effect until terminated hereunder. This agreement shall terminate automatically on Licensee's failure to comply with any of the provisions herein, including any attempt to transfer this license or the Software or Documentation. Upon any termination, Licensee shall promptly destroy or return to Redback all copies of the Software and Documentation, including all original and archival copies. No refunds shall be given for such returned materials. Notwithstanding any termination of this License, the rights and obligations relating to title, warranty, termination and limitation of liability, as well as any other provisions which survive by their terms, shall survive termination:

Restricted Rights. The Software and Documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software—Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Redback Networks Inc., 1195 Borregas Avenue, Sunnyvale, California 94089.

Miscellaneous. Licensee may not assign or transfer any of its rights or delegate any of its obligations under this agreement. No delay, failure or waiver by either party to exercise any right or remedy under this agreement shall operate to waive any exercise of such right or remedy or any other right or remedy. This agreement shall be governed by and construed in accordance with the laws of the State of California without regard to conflict of laws principles and without regard to the 1980 U.N. Convention on Contracts for the International Sale of Goods. If any provision in this agreement shall be found or be held to be invalid or unenforceable, then the meaning of said provision shall be construed, to the extent feasible, so as to render the provision enforceable, and the remainder of this agreement shall remain in full force and effect. This agreement constitutes the entire agreement between Licensee and Redback with respect to the subject matter of this agreement.

Proprietary Notices. Licensee shall maintain and reproduce all copyright and other proprietary notices on all copies of the Software in the same form and manner that such notices are included on the Software. The following third party Software may be included with your product and is subject to this software license agreement. All rights in copyright are reserved to the copyright owner:

SNMP Monolithic Agent. © 1992–1998 SNMP Research International, Inc.

VxWorks. © 1984–1998 Wind River Systems, Inc.

Redback adaptation and implementation of the UDP and TCP protocols developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. © 1982, 1986, 1988, 1990, 1993, 1995 The Regents of the University of California. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the University of California, Berkeley and its contributors."

Point-to-Point Protocol (PPP). © 1989 Carnegie-Mellon University.

Dynamic Host Configuration Protocol (DHCP) © 1997, 1998 The Internet Software Consortium.

Portions of the Redback Access Operating System (AOS) use cryptographic software written by Eric Young (eay@cryptsoft.com).

SSH IPSEC Technology (pat.pending). © 1995–2000 SSH Communications Security Ltd. (www.ssh.fi).

Neither the name of any third party Software developer nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission of such third party.

Limitation of Liability and Damages

THE FOLLOWING LIMITATION OF LIABILITY AND DAMAGES APPLIES TO ALL HARDWARE, SOFTWARE AND DOCUMENTATION SOLD, LICENSED OR OTHERWISE DISTRIBUTED BY REDBACK OR ITS RESELLERS.

IN NO EVENT SHALL REDBACK, ITS SUPPLIERS OR ITS DISTRIBUTORS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGE, INCLUDING WITHOUT LIMITATION LOSS OF DATA, LOST PROFITS OR COST OF COVER, ARISING FROM THE USE OF THE HARDWARE, SOFTWARE OR DOCUMENTATION OR ANY DEFECT IN THE HARDWARE, SOFTWARE OR DOCUMENTATION, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION SHALL APPLY EVEN IF REDBACK, ITS SUPPLIERS OR ITS DISTRIBUTOR SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGE. IN PARTICULAR, BUT WITHOUT LIMITATION, REDBACK, ITS SUPPLIERS AND ITS DISTRIBUTORS SHALL HAVE NO LIABILITY FOR THE LOSS OF ANY INFORMATION STORED OR COMMUNICATED OR ATTEMPTED TO BE STORED OR COMMUNICATED WITHIN ANY REDBACK SYSTEM USING THE HARDWARE OR SOFTWARE.

THE MAXIMUM AGGREGATE LIABILITY OF REDBACK AND ITS SUPPLIERS FOR ANY CLAIM ARISING OUT OF USE OF THE HARDWARE, SOFTWARE OR DOCUMENTATION OR ANY DEFECT IN THE HARDWARE, SOFTWARE OR DOCUMENTATION, ON ANY AND ALL THEORIES OF LIABILITY, INCLUDING WITHOUT LIMITATION NEGLIGENCE BY REDBACK, SHALL IN ALL EVENTS BE LIMITED TO RETURN OF THE AMOUNTS ACTUALLY PAID TO REDBACK FOR THE DEFECTIVE HARDWARE OR SOFTWARE, LESS DEPRECIATION OF SUCH AMOUNTS LINEARLY OVER A THREE-YEAR PERIOD, WHICH THE PARTIES AGREE CONSTITUTES A REASONABLE RATE OF DEPRECIATION.

FCC Notice

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

1. MODIFICATIONS

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Redback could void the user's authority to operate the equipment.

2. CABLES

Connection to this device must be made with shielded cables with metallic RFI/EMI connector hoods to maintain compliance with FCC Rules and Regulations.

3. POWER CORD SET REQUIREMENTS

The power cord set used with the System must meet the requirements of the country, whether it is 100-120 or 220-264 VAC. For the U.S. and Canada, the cord set must be UL Listed and CSA Certified and suitable for the input current of the system.

For DC-powered systems, the installation instructions need to be followed.

VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Safety Notices

1. Laser Equipment:

CAUTION! USE OF CONTROLS OR ADJUSTMENTS OF PERFORMANCE OR PROCEDURES OTHER THAN THOSE SPECIFIED HEREIN MAY RESULT IN HAZARDOUS RADIATION EXPOSURE.

Class 1 Laser Product
Product is certified by the manufacturer to comply with DHHS Rule 21 Subchapter J.

CAUTION! INVISIBLE LASER RADIATION WHEN AN OPTICAL INTERFACE IS OPEN.

2. Lithium Battery Warnings:

It is recommended that, when required, Redback replace the lithium battery.

WARNING! Do not mutilate, puncture, or dispose of batteries in fire. The batteries can burst or explode, releasing hazardous chemicals. Discard used batteries according to the manufacturer's instructions and in accordance with your local regulations.

Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer's instructions.

VARNING Eksplosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

ADVARSEL! Lithiumbatteri—Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage tilleverandøren.

VARIOTUS Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan valmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mikaisesti.

ADVARSEL Eksplosjonsfare ved feilaktig skifte av batteri. Benytt samme batteritype eller en tilsvarende type anbefait av apparatfabrikanten. Brukte batterier kasseres i henhold til fabrikantens instruksjoner.

WAARSCHUWING! Bij dit produkt zijn batterijen geleverd. Wanneer deze leeg zijn, moet u ze niet weggooien maar inleveren als KCA.

Table of Contents

About This Guide xxiii
Objectives xxiii
Related Publications xxiii
Intended Audience xxiii
Organization xxiv
Conventions xxv
Commands xxv
Examples xxvi

Part 1: Getting Started

Chapter 1: System Overview 1-1
The Redback Solution 1-1
AOS Concepts 1-4

Chapter 2: User Interface Commands 2-1
? (help) 2-2
enable 2-4
end 2-6
exit 2-7
show privilege 2-8

Chapter 3: Terminal Settings and Telnet Commands 3-1
administrator reserve 3-2
clear tty 3-4
console-break-enable 3-5
debug ip telnet 3-6
debug sshd 3-8
length 3-9
line 3-11
show administrator reservations 3-12
show terminal 3-13
sshd keygen 3-14
telnet 3-15
terminal length 3-17
terminal monitor 3-18
terminal width 3-20
width 3-21

Chapter 4: System Image and Configuration File Commands 4-1
boot configuration 4-2
boot system 4-4
configure 4-6
copy 4-8
debug ip tftp 4-11
delete 4-13
directory 4-15
fabric revert 4-17
format 4-19
mkdir 4-21
module extract 4-23
reload 4-25
rename 4-27
rmdir 4-29
save configuration 4-31
show configuration 4-33
show version 4-35

Chapter 5: Basic System Commands 5-1
banner motd 5-2
clock set 5-3
clock summer-time 5-4
clock timezone 5-6
configure 5-8
privilege 5-10
show clock 5-12
system contact 5-13
system hostname 5-14
system location 5-15

Part 2: Setting Up Contexts with Interfaces and Subscribers

Chapter 6: Context Commands 6-1
administrator 6-2
clear ip counter 6-4
context 6-5
domain 6-7
ip access-group 6-9
operator 6-11
privilege max 6-13
privilege start 6-14
show context 6-15
show ip host 6-17
show ip traffic 6-19
show privilege 6-21
timeout 6-22

Chapter 7: Interface Commands 7-1
debug ip arp 7-2
debug ip interface 7-4
debug ip secured-arp 7-6
description 7-8

interface 7-9
ip address 7-11
ip arp arpa 7-14
ip arp timeout 7-15
ip ignore-df-bit 7-16
ip lookup host 7-18
ip mask-reply 7-20
ip mtu 7-21
ip pool 7-22
ip secured-arp 7-24
ip source-address 7-26
show ip arp 7-27
show ip interface 7-29
show ip pool 7-32
show ip secured-arp 7-33

Chapter 8: Subscriber Commands 8-1
clear arp-cache 8-2
clear subscriber 8-3
debug ip arp 8-5
ip address 8-6
ip arp 8-8
ip source-validation 8-10
ip tos-field 8-11
outbound password 8-13
password 8-14
police 8-15
port-limit 8-16
rate-limit 8-17
show ip arp 8-18
show subscribers 8-20
subscriber 8-23
timeout 8-25

Part 3: Ports, Circuits, Channels, and Bindings

Chapter 9: Common Port, Circuit, and Channel Commands 9-1
buffers 9-2
bulkstats schema 9-4
clear circuit 9-7
clear port counters 9-9
clear port dot1q 9-11
debug hdlc 9-12
description 9-14
ip host 9-15
mac address 9-17
police 9-19
rate-limit 9-20
show port counters 9-21
show port diag 9-29
show port dot1q 9-31
show port info 9-33
show port table 9-35

shutdown 9-37

Chapter 10: Ethernet Port Commands 10-1
encapsulation 10-2
ip host 10-4
loopback 10-6
medium 10-7
port ethernet 10-9
radius attribute medium-type 10-11

Chapter 11: ATM Port Commands 11-1
8khztiming 11-2
cablelength 11-3
cell-delineation 11-5
clock-source 11-6
fdl 11-7
framing 11-9
idle-cell 11-11
length 11-13
linecode 11-14
loopback 11-15
port atm 11-16
scramble 11-17
yellow-alarm 11-18

Chapter 12: Channelized DS-3 Port Commands 12-1
bert 12-2
clear bert 12-4
clear pmon 12-5
clock-source 12-6
crc 12-7
encapsulation 12-8
fdl 12-10
framing 12-11
hdlc-channel 12-13
invert-data 12-14
keepalive 12-15
length 12-16
loopback 12-17
port channelized-ds3 12-19
show bert 12-20
show hdlc-channel counters 12-21
show hdlc-config 12-23
show pmon 12-25
show t1 info 12-28
speed 12-30
t1 12-31
yellow-alarm 12-32

Chapter 13: Clear-Channel DS-3 and Clear-Channel E3 Port Commands 13-1
clock-source 13-2
encapsulation 13-3
framing 13-5
keepalive 13-6

length . . . 13-8
loopback . . . 13-9
port ds3 . . . 13-11
port e3 . . . 13-12

Chapter 14: HSSI Port Commands . . . 14-1
encapsulation . . . 14-2
hardware-interface . . . 14-4
keepalive . . . 14-6
loopback . . . 14-8
port hssi . . . 14-10

Chapter 15: Packet T1 and Packet E1 Port Commands . . . 15-1
bert . . . 15-2
cablelength . . . 15-4
clear bert . . . 15-6
clear pmon . . . 15-7
clock-source . . . 15-8
encapsulation . . . 15-9
fdl . . . 15-11
framing . . . 15-12
invert-data . . . 15-14
keepalive . . . 15-15
linecode . . . 15-17
loopback . . . 15-18
port ds1 . . . 15-19
port e1 . . . 15-20
show bert . . . 15-21
show pmon . . . 15-22
show t1 info . . . 15-24
speed . . . 15-26
timeslot . . . 15-27
ts16 . . . 15-29
yellow-alarm . . . 15-30

Chapter 16: Packet over SONET Port Commands . . . 16-1
c2byte . . . 16-2
clock-source . . . 16-4
crc16 . . . 16-5
encapsulation . . . 16-6
framing sdh . . . 16-8
loopback . . . 16-9
packet-length . . . 16-11
port pos . . . 16-12
scramble . . . 16-13

Chapter 17: ATM Commands . . . 17-1
atm ping . . . 17-2
atm profile . . . 17-4
atm pvc . . . 17-5
atm pvc explicit . . . 17-8
atm pvc on-demand . . . 17-11
buffers . . . 17-14
bulkstats schema . . . 17-16

clock mode 17-19
clock source 17-21
clpbit 17-23
counters 17-24
debug atm 17-26
delay-tolerance 17-28
description 17-29
frame-length 17-30
ima enable 17-31
ima group 17-32
minimum-links 17-33
ports 17-34
radius attribute medium-type 17-36
shaping 17-38
show atm counters 17-40
show atm multicast 17-43
show atm profile 17-47
show atm pvc 17-49
show ima group 17-52
show ima pmon 17-54
symmetry 17-57

Chapter 18: Frame Relay Commands 18-1
buffers 18-2
bulkstats schema 18-3
clear lmi-counters 18-6
counters 18-8
debug frame-relay lmi 18-10
debug frame-relay packet 18-12
frame-relay auto-detect 18-14
frame-relay intf-type 18-16
frame-relay keepalive 18-18
frame-relay lmi-n391dte 18-20
frame-relay lmi-n392dce 18-22
frame-relay lmi-n392dte 18-24
frame-relay lmi-n393dce 18-26
frame-relay lmi-n393dte 18-28
frame-relay lmi-t392dce 18-30
frame-relay lmi-type 18-32
frame-relay profile 18-34
frame-relay pvc 18-35
frame-relay pvc explicit 18-38
frame-relay pvc on-demand 18-41
frame-relay-test 18-44
radius attribute medium-type 18-46
show frame-relay counters 18-48
show frame-relay lmi-config 18-51
show frame-relay lmi-errors 18-53
show frame-relay lmi-stats 18-55
show frame-relay multicast 18-57
show frame-relay profile 18-60
show frame-relay pvc 18-62

Chapter 19: 802.1Q Commands 19-1
description 19-2
dot1q profile 19-3
dot1q pvc 19-4
pbit-setting 19-6
show dot1q counters 19-7
show dot1q profile 19-9
show dot1q pvc 19-10

Chapter 20: Bind Commands 20-1
bind authentication 20-2
bind auto-subscriber 20-4
bind bypass 20-7
bind dot1q 20-9
bind interface 20-11
bind l2tp-tunnel 20-13
bind multi 20-15
bind session 20-18
bind subscriber 20-20
show bindings 20-22

Part 4: Bridges and Bypasses

Chapter 21: Bridging Commands 21-1
bridge 21-2
bridge-group 21-4
bridge-only 21-6
bridge station-move verbose 21-8
clear bridge table 21-10
debug bridge span-tree 21-11
debug bridge table 21-13
forward-time 21-14
hello-time 21-16
max-age 21-17
priority 21-18
protocol 21-20
show bridge address 21-22
show bridge info 21-23
show bridge span-tree 21-24
show bridge table 21-27

Chapter 22: Bypass Commands 22-1
bypass 22-2
description 22-4
show bypass 22-5

Part 5: Point-to-Point Protocol

Chapter 23: PPP and PPPoE Commands 23-1
debug ppp 23-2
debug pppoe 23-5

debug ip ppp-proxy-arp . . . 23-7
interface . . . 23-9
ip ppp-proxy-arp . . . 23-11
port-limit . . . 23-13
ppp compression . . . 23-15
ppp keepalive . . . 23-16
ppp mtu . . . 23-18
ppp multilink enable . . . 23-19
ppp multilink endpoint-discriminator . . . 23-21
ppp multilink mrru . . . 23-23
ppp our-options . . . 23-24
ppp passive . . . 23-26
ppp peer-options . . . 23-28
pppoe client . . . 23-30
pppoe motm . . . 23-32
pppoe services . . . 23-34
pppoe tag . . . 23-35
pppoe url . . . 23-37
show ip ppp-proxy-arp . . . 23-39
show ppp . . . 23-41
show ppp compression . . . 23-44
show ppp multilink . . . 23-46
show pppoe . . . 23-48
show pppoe counters . . . 23-50
show pppoe services . . . 23-52

Part 6: Tunnels

Chapter 24: GRE Commands . . . 24-1
checksum . . . 24-2
clear gre peer . . . 24-3
description . . . 24-5
gre-circuit creation . . . 24-6
gre-peer . . . 24-7
gre-rpf-check . . . 24-9
gre-tunnel . . . 24-10
ip host . . . 24-12
police . . . 24-14
rate-limit . . . 24-16
show gre counters . . . 24-18
show gre info . . . 24-20
show gre tunnel counters . . . 24-22
show gre tunnel info . . . 24-23
tunnel map . . . 24-25

Chapter 25: L2TP Commands . . . 25-1
algorithm . . . 25-2
clear tunnel . . . 25-6
deadtime . . . 25-8
debug l2x . . . 25-10
description . . . 25-12
dnis . . . 25-14
domain . . . 25-16

ethernet encapsulation 25-18
ethernet session 25-19
function 25-21
ipsec peer 25-23
l2tp-group name 25-24
l2tp attribute calling-number real-circuit-id 25-26
l2tp-peer default 25-27
l2tp-peer name 25-29
l2tp-peer unnamed 25-31
l2tp radius auto-group 25-33
l2x profile 25-35
l2tp eth-sess-idle-timeout 25-37
local-name 25-39
max-sessions 25-41
max-tunnels 25-43
min-subscribers 25-45
peer-name 25-46
police 25-48
profile 25-50
rate-limit 25-52
retry 25-54
secondary-tunnel-auth 25-56
session-auth 25-58
show l2tp counters 25-60
show l2tp group 25-67
show l2tp info 25-69
static 25-77
timeout 25-79
tunnel-auth 25-81
tunnel domain 25-83
tunnel name 25-85
tunnel-window 25-86

Chapter 26: L2F Commands 26-1
clear tunnel 26-2
debug l2x 26-4
description 26-6
domain 26-8
function 26-10
l2f-peer name 26-12
l2x profile 26-14
local-name 26-16
max-sessions 26-18
max-tunnels 26-20
min-subscribers 26-21
police 26-22
profile 26-24
rate-limit 26-26
retry 26-28
session-auth 26-30
show l2f counters 26-32
show l2f info 26-35
timeout 26-37
tunnel-auth 26-39

tunnel domain 26-41
tunnel name 26-43

Part 7: Security

Chapter 27: IPSec Commands 27-1
ah hash 27-2
cipher 27-4
clear ipsec peer 27-5
debug ipsec ike 27-7
debug ipsec peer 27-8
encapsulation-mode 27-10
esp cipher 27-12
esp hash 27-14
hash 27-16
ike auth 27-17
ike group 27-18
ike lifetime hard kbytes 27-19
ike lifetime hard seconds 27-21
ike lifetime soft kbytes 27-23
ike lifetime soft seconds 27-25
ike pre-shared-key 27-27
ike sa_subnet 27-28
in 27-30
ip-address local 27-31
ip-address remote 27-32
ipsec key name 27-33
ipsec lifetime hard kbytes 27-35
ipsec lifetime soft kbytes 27-37
ipsec lifetime hard seconds 27-39
ipsec lifetime soft seconds 27-41
ipsec mode 27-43
ipsec options 27-44
ipsec peer default 27-45
ipsec peer name 27-47
ipsec pfs-group 27-48
ipsec policy name 27-50
ipsec proposal crypto name 27-51
ipsec proposal ike name 27-52
ipsec tunnel policy 27-53
out 27-54
port te 27-56
proposal crypto 27-57
proposal ike 27-59
show ipsec peer 27-60
show ipsec stats 27-62
show te cpu 27-65
show te performance 27-67
show te ps 27-68
show te time 27-70
spi in 27-71
spi out 27-72
tunnel ip 27-73

Part 8: IP Services

Chapter 28: DNS Commands 28-1
clear ip localhosts 28-2
debug ip dns 28-3
dns 28-5
ip dns-ttl 28-7
ip domain-lookup 28-8
ip domain-name 28-10
ip localhost 28-11
ip name-servers 28-13
show ip localhosts 28-15

Chapter 29: DHCP Commands 29-1
debug dhcp 29-2
dhcp max-addrs 29-4
dhcp preserve-state 29-6
dhcp relay option 29-8
dhcp relay server 29-10
dhcp relay size 29-12
dhcp server default-lease-time 29-14
dhcp server filename 29-15
dhcp server max-lease-time 29-16
dhcp server next-server 29-17
dhcp server option 29-18
dhcp server range 29-20
format 29-21
show dhcp 29-23
show dhcp server lease 29-26
show dhcp server sram 29-28

Chapter 30: NTP Commands 30-1
debug ntp 30-2
ntp mode 30-4
ntp server 30-5
show ntp associations 30-7
show ntp status 30-9
slowsync 30-11

Part 9: Routing

Chapter 31: Basic IP Routing Commands 31-1
debug ip irdp 31-2
debug ip route 31-4
debug ip routing 31-6
ip irdp 31-8
ip maximum-paths 31-10
ip route 31-12
show ip route 31-16
show ip static-route 31-19

Chapter 32: RIP Commands 32-1
auto-summary 32-2
debug ip rip 32-3
ip rip interface-cost 32-5
ip rip listen 32-7
ip rip receive version 32-8
ip rip send version 32-10
ip rip split-horizon 32-12
ip rip supply 32-13
network 32-14
precedence 32-16
redistribute 32-18
router rip 32-20
version 32-21

Chapter 33: OSPF Commands 33-1
area 33-2
area-sumrange 33-4
areatype 33-6
as-sumrange 33-8
authentication 33-10
cost 33-12
debug ip ospf 33-13
default-originate 33-15
defaultroute 33-17
hello-interval 33-19
nssa-sumrange 33-21
ospf-interface 33-23
precedence 33-25
redistribute 33-27
retransmit-interval 33-29
routerdead-interval 33-30
router-id 33-32
router ospf 33-33
router-priority 33-34
show ip ospf 33-35
show ip ospf area 33-37
show ip ospf border-router 33-39
show ip ospf database 33-41
show ip ospf interface 33-45
show ip ospf neighbor 33-47
show ip ospf summary-range 33-49
spf-timers 33-52
transmit-delay 33-54

Chapter 34: BGP Commands 34-1
accept-med 34-2
aggregate-address 34-4
allow-bad-routerid 34-6
always-compare-med 34-7
clear ip bgp 34-9
client-to-client 34-11
cluster-id 34-12
debug ip bgp 34-13

default-originate 34-15
enable-peer 34-16
export-non-active 34-17
group 34-18
hold-time 34-20
maximum-prefix 34-22
maximum-prefix-warn 34-24
metric-out 34-26
neighbor 34-28
nexthop-self 34-29
no-aggregator-id 34-31
out-delay 34-33
passive 34-35
precedence 34-37
preference 34-39
redistribute 34-41
remove-private-AS 34-43
route-map 34-45
router bgp 34-47
router-id 34-49
route-reflector-client 34-50
show ip bgp 34-52
show ip bgp groups 34-55
show ip bgp neighbors 34-57
show ip bgp paths 34-60
show ip bgp summary 34-62
throttle 34-64
ttl 34-65

Chapter 35: Routing Policy Commands 35-1
as-path access-list 35-2
community-list 35-5
ip bgp-community 35-7
match as-path 35-8
match community-list 35-9
match interface 35-10
match ip address 35-11
match ip next-hop 35-12
match metric 35-13
match route-type 35-14
match tag 35-16
route-access-list *extended-access-list-num* 35-17
route-access-list *standard-access-list-num* 35-19
route-map 35-21
set as-path prepend 35-23
set community 35-25
set ip next-hop 35-27
set local-preference 35-29
set metric 35-30
set origin 35-32
set preference 35-33
show as-path-access-list 35-34
show community-list 35-35
show route-access-list 35-36

show route-map 35-37

Chapter 36: IGMP Proxy Commands 36-1
debug ip igmp 36-2
def-version 36-4
ip igmp 36-6
ip igmp join-group 36-8
ip igmp leave-group 36-11
ip igmp mode 36-14
ip multicast max-groups 36-15
ip multicast receive 36-17
ip multicast-routing 36-19
ip multicast send 36-21
last-member-query-interval 36-23
query-interval 36-25
query-response-interval 36-27
robustness 36-29
router-igmp-interface 36-31
router igmp-proxy 36-33
show ip igmp 36-34
startup-query-interval 36-40
unsolicited-report-interval 36-42
version1-router-interval 36-44

Part 10: Access Control Lists

Chapter 37: IP Access Control List Commands 37-1
aaa authorization access-list 37-3
access-list undefined 37-5
clear access-list 37-7
ip access-group 37-9
ip access-list 37-11
ip dynamic-acl timeout 37-13
ip reflexive timeout 37-15
{permit | deny} 37-16
{permit | deny} icmp 37-18
{permit | deny} igmp 37-21
{permit | deny} ip 37-24
{permit | deny} {tcp | udp} 37-26
redirect *interface next-hop* 37-29
redirect *interface next-hop* icmp 37-34
redirect *interface next-hop* ip 37-39
redirect *interface next-hop* {tcp | udp} 37-44
reflexive {ftp | tftp} 37-50
reflexive {tcp | udp} 37-53
show ip access-list 37-57
show ip dynamic-acl subscriber 37-59
show ip reflexive-acl 37-61

Chapter 38: Bridge Access Control List Commands 38-1
access-list undefined 38-3
bridge access-list 38-5
bridge-group 38-6

{permit | deny} 38-8
{permit | deny} lsap 38-11
{permit | deny} type 38-13
show bridge access-list 38-15

Chapter 39: Service Access List Commands 39-1
{permit | deny} any 39-3
{permit | deny} context 39-5
{permit | deny} domain 39-7
service access-list 39-9
show service access-list 39-11

Part 11: AAA and RADIUS

Chapter 40: AAA Commands 40-1
aaa accounting 40-2
aaa authentication administrator 40-4
aaa authentication re-try 40-5
aaa authentication subscriber 40-7
aaa authorization access-list 40-9
aaa authorization circuit 40-11
aaa authorization gre 40-12
aaa authorization tunnel 40-13
aaa binding 40-15
aaa default-domain 40-17
aaa delay-start-record 40-21
aaa hint ip-address 40-22
aaa last-resort 40-24
aaa max-subscribers 40-26
aaa min-subscribers 40-28
aaa terse-messages 40-30
aaa update 40-31
aaa username-format 40-33
debug aaa 40-35
show username-format 40-37

Chapter 41: RADIUS Commands 41-1
debug radius 41-2
radius accounting algorithm 41-4
radius accounting deadtime 41-6
radius accounting max-outstanding 41-7
radius accounting max-retries 41-9
radius accounting server 41-11
radius accounting timeout 41-13
radius algorithm 41-15
radius attribute acct-session-id 41-17
radius attribute calling-station-id 41-19
radius attribute connect-info 41-21
radius attribute filter-id 41-23
radius attribute medium-type 41-25
radius attribute nas-ip-address 41-27
radius attribute non-rfc-242 41-29
radius attribute tunnel password 41-31

radius deadtime 41-33
radius max-outstanding 41-35
radius max-retries 41-37
radius server 41-39
radius strip-domain 41-41
radius timeout 41-43
show radius counters 41-45

Part 12: System Management

Chapter 42: System Monitoring and Testing Commands 42-1
clear administrator 42-2
clear circuit 42-3
clear fabric counters 42-5
clear subscriber 42-6
debug all 42-7
debug ip all 42-10
debug ip ce-fe 42-12
debug ip host 42-13
debug ip icmp 42-15
debug ip packet 42-17
debug ip sm-cm 42-19
debug ip tcp 42-21
fabric test 42-23
ping 42-24
show administrators 42-26
show cm stats 42-28
show cm table 42-33
show debugging 42-35
show diag 42-37
show envmon 42-41
show fabric counters 42-42
show fabric table 42-44
show fe stats 42-47
show hardware 42-52
show ip socket 42-56
show ip traffic 42-57
show memory 42-59
show process 42-61
show slot 42-63
show sram 42-64
show stack 42-66
show subscribers 42-67
show tech 42-70
traceroute 42-72

Chapter 43: Bulk Statistics Commands 43-1
bulkstats collection 43-2
bulkstats force transfer 43-4
bulkstats mode 43-5
bulkstats schema 43-6
header format 43-10
limit 43-12

localdir 43-14
receiver 43-16
remotefile 43-18
sample-interval 43-20
schema 43-21
schema-dump 43-24
schema profile 43-25
show bulkstats 43-28
transfer-interval 43-30

Chapter 44: Logging Commands 44-1
log checkpoint 44-2
logging console 44-3
logging filter 44-5
logging syslog 44-9
save log 44-11
show log 44-13
show logging 44-17

Part 13: Network Management Services

Chapter 45: SNMP and RMON Commands 45-1
debug snmp 45-2
rmon alarm 45-4
rmon event 45-6
show snmp 45-8
show snmp server 45-10
snmp community 45-12
snmp engine-id 45-14
snmp group 45-16
snmp notify 45-18
snmp notify-filter 45-20
snmp notify-target 45-22
snmp server 45-24
snmp target 45-26
snmp target-parameters 45-29
snmp user 45-31
snmp view 45-33

Chapter 46: Web Management Commands 46-1
clear http 46-2
http server 46-3

Chapter 47: NetOp Commands 47-1
netop server 47-2

Part 14: Appendixes

Appendix A: Obsolete Commands A-1

Part 15: Indexes

Commands by Mode Index 1

Index 1

About This Guide

Objectives

This document provides syntax description and usage guidelines for all Access Operating System (AOS) commands. These commands are used to configure, operate, and maintain the Subscriber Management System (SMS) device.

Note Each SMS platform supports a distinct set of modules and ports. For example, the SMS 10000 contains Connection Manager (CM) and System Manager (SM) modules, where the SMS 500, SMS 1000, and SMS 1800 have Forwarding Engine (FE) modules and Control Engine (CE) modules. This guide provides commands for all Redback products, including platform-specific commands, such as **show fe stats** and **show cm stats**, and commands with variables that are specific to a particular platform.

Related Publications

Use this guide in conjunction with the *Access Operating System (AOS) Configuration Guide*. The configuration guide provides a technical overview, configuration tasks, and configuration examples for all AOS features.

Intended Audience

This publication is intended for system and network administrators experienced in access and internetwork administration.

Organization

This guide is organized as follows:

- Part 1. Getting Started

  Provides an overview and describes the commands used to access the AOS, to load system images and configuration files, and to configure basic system parameters.

- Part 2. Setting Up Contexts with Interfaces and Subscribers

  Describes the commands used to configure the local context and multiple contexts, and to set up accounts for the operators and administrators who maintain one or more contexts. Provides the commands needed to configure the interfaces and subscriber associated with a specific context.

- Part 3. Ports, Circuits, Channels, and Bindings

  Describes the commands needed to configure common port, circuit, and channel elements, and port-specific commands. Provides the commands that configure Asynchronous Transfer Mode (ATM) and Frame Relay features, including profiles that can be easily applied to multiple ports. Provides the commands used to bind circuits, channels, or ports to interfaces, subscribers, Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) peers, L2TP groups, or bypasses.

- Part 4. Bridges and Bypasses

  Provides the commands that configure media access control (MAC)-based (transparent) and IEEE 802.1D Spanning-Tree Protocol bridges. Describes the commands that are used to configure bypasses, which bind two circuits, channels, or ports together without protocol translation.

- Part 5. Point-to-Point Protocol

  Provides the commands needed to configure Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE).

- Part 6. Tunnels

  Supplies the commands needed to configure GRE, L2TP, or L2F tunnels and peers.

- Part 7. Security

  Describes the AOS commands that configure IP Security (IPSec) on an SMS device equipped with at least one IPSec/Compression Transform Engine (TE) module.

- Part 8. IP Services

  Describes how the AOS interacts with Dynamic Host Configuration Protocol (DHCP), Domain Naming System (DNS) servers, and Network Time Protocol (NTP) servers.

- Part 9. Routing

  Explains the commands that configure static IP, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) routing. Describes the commands that configure routing polices. Provides the commands needed to configure Internet Group Management Protocol (IGMP) proxy, which allows the SMS device to forward IP multicast traffic without running a multicast routing protocol.

- Part 10. Access Control Lists

  Provides information on how to configure IP and bridging access control lists, and service access lists, which restrict subscriber access to contexts and domains on a per-circuit basis.

- Part 11. AAA and RADIUS

  Describes the commands needed to configure global or context-specific authentication, authorization, and accounting (AAA) and Remote Authentication Dial-In User Service (RADIUS) features. Subscriber AAA can be accomplished through local configuration of subscriber records or through a remote RADIUS server. Circuits can be created on demand via RADIUS for a specific context. The AAA configuration of the specified context is used to configure the profile, encapsulation, and binding of each circuit.

- Part 12. System Management

  Describes the commands used to monitor and test system-wide parameters, including administrators, hardware, memory, processes, and so on. Describes the commands that enable the AOS to collect system statistics (bulkstats) and to transfer and store the collected data on remote servers. Describes the commands that configure system event logging.

- Part 13. Network Management

  Explains the commands used to configure Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) features, to access the AOS from a web browser, and to configure the NetOp server port on the SMS device that is used to communicate with the NetOp Network Manager product.

- Part 14. Appendixes

  Provides a list of obsolete commands and the new commands that replace them.

- Part 15. Indexes

  Provides a commands-by-mode index and an alphabetical index.

Conventions

Commands

Command descriptions use the following conventions:

- Commands and keywords are indicated in **boldface**.
- Arguments where you must supply the value are indicated in *italics*.
- Optional constructs within commands, and constructs that are not used in all cases are shown in square brackets ([ ]).
- Alternative parameters within commands are separated by vertical bars (|).
- Alternative, but required parameters, are shown within grouped braces ({ }), and are separated by vertical bars (|).

Examples

Examples use the following conventions:

- System prompts are of the form `[context]hostname(mode)#` for interactive sessions. Here, the context is the current context in which operator and administrator commands are applied, the hostname is the configured name of the Redback system, and the mode is a string indicating the current configuration mode, if applicable. For example, the prompt in context configuration mode is `[local]RedBack(config-ctx)#`.
- Information displayed by the system is in `Courier` font.
- Information that you should enter is in **`boldface Courier`** font.

Part 1

Getting Started

System Overview

This chapter describes the Access Operating System (AOS) software, including where our products fit in today's high-speed access networks, an overview of AOS concepts and terminology, and an overview of the AOS configuration process.

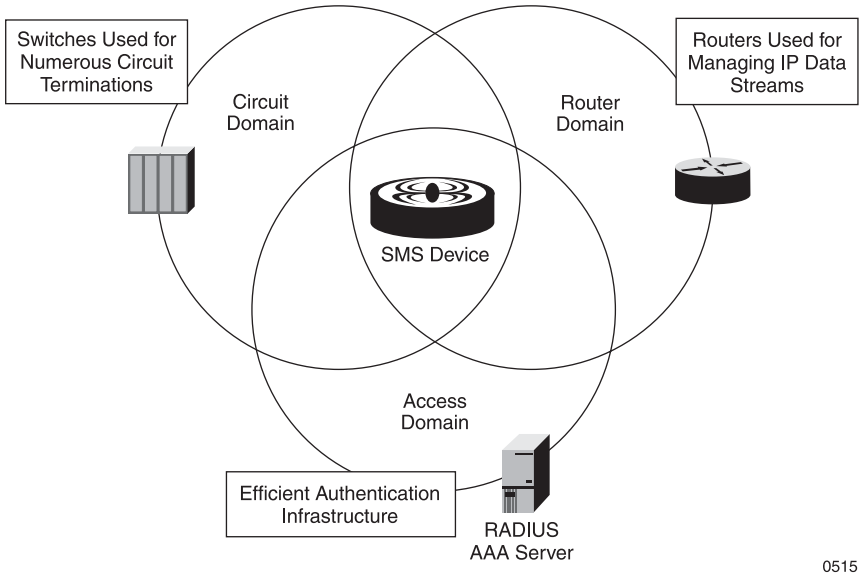
The Redback Solution

Modern networks have grown to the point where general-purpose devices can no longer handle all of the complex functions necessary to deliver emerging high-speed services. Increasingly, service providers have partitioned their networks into access functions and backbone functions. The our products, including the Subscriber Management System (SMS) hardware and the AOS software, bridge the gap between high-speed access methods, such as digital subscriber line (DSL), cable, and wireless, and the Internet backbone.

AOS Functions

The AOS software provides effective circuit termination, access functions, and routing in a single system. Figure 1-1 illustrates the functional areas of our products.

Figure 1-1 AOS Functions



The AOS provides the following functions:

- Circuit termination—the AOS provides effective circuit termination for all major high-speed access methods. Whether deployed by carriers, cable operators, or service providers, the AOS accepts a large concentration of high-speed data traffic from such devices as DSL access multiplexors (DSLAMs), cable modem termination systems, and wireless termination systems. The AOS offloads the circuit termination function from routers connecting to the Internet backbone, reducing the processing requirements for these routers and providing a scalable solution. The AOS supports up to 10,000 subscribers.
- Access—the AOS provides access functionality that traditional routers were not designed to provide, such as subscriber management, provisioning, authentication and accounting. The AOS supports service providers' existing accounting and management software systems, enabling service providers to quickly deploy new high-speed access services.
- Routing—the AOS provides routing of subscriber traffic based on layer 3 addressing. The AOS performs all translations necessary to convert subscriber traffic to IP, relieving the service provider backbone routers of frame translations that can cause congestion on high-volume routers. The AOS grooms individual subscriber data streams into simplified IP flows for routers connecting to the Internet backbone.

AOS Features

The AOS is an advanced operating system designed to optimize subscriber management and routing functions. Some of the key features that the AOS software supports include:

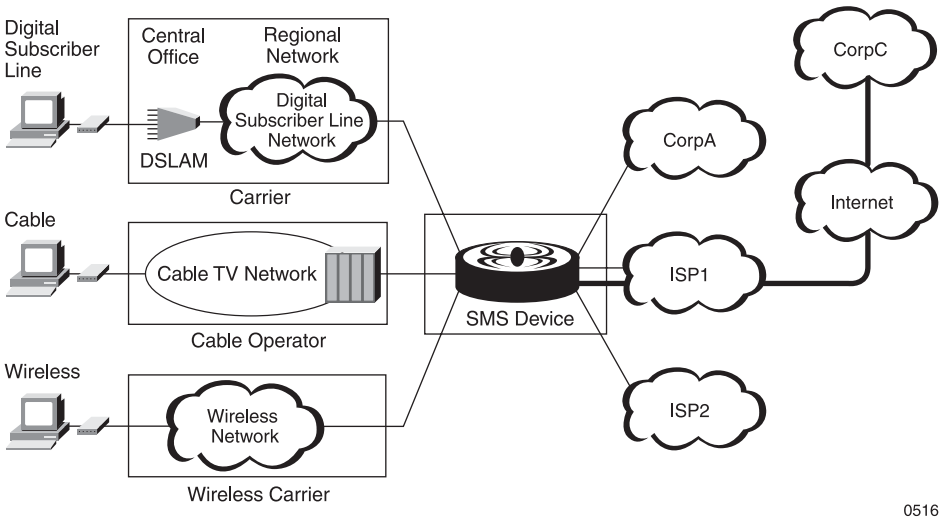
- Dynamic service selection—the AOS supports the unique capability to dynamically bind subscriber sessions to services. This capability enables dynamic service selection to be deployed by carriers and service providers alike.

- Layer 2 Tunneling Protocol (L2TP)—the AOS supports L2TP, the standard method of building a Virtual Private Network (VPN) that enables fixed and mobile users to simulate a private network using a shared infrastructure, such as the Internet. VPNs also enable mobile users to make secure connections to their corporate intranets or extranets over the public Internet.
- Traffic management—the AOS supports traffic management features, including policing and rate-limiting, to support the creation of different service classes and provide service providers with predictable traffic behavior for better management of their networks.
- Routing protocol support—the AOS includes support for various popular routing protocols.
- IP multicast—the AOS supports Internet Group Multicast Protocol (IGMP) proxy functionality.
- Web-based management—The Web-based management capabilities in the AOS allow service providers to streamline operations and simplify troubleshooting through a common, easy-to-use browser interface.
- Bulk statistics—The bulk statistics capabilities in the AOS allow service providers access to information that enables them to provide efficient storage and transfer of high volume accounting data.

AOS Applications

Figure 1-2 illustrates how the Subscriber Management System (SMS) device provides access services for different types of high-speed access methods, including DSL, cable, and wireless. It also illustrates the SMS device being used to provide access to multiple networks, including two corporate networks (CorpA and CorpC), and two service provider networks (ISP1 and ISP2). In this example, ISP1 provides a VPN service for CorpC using a tunnel. All of these features can be implemented using a single system.

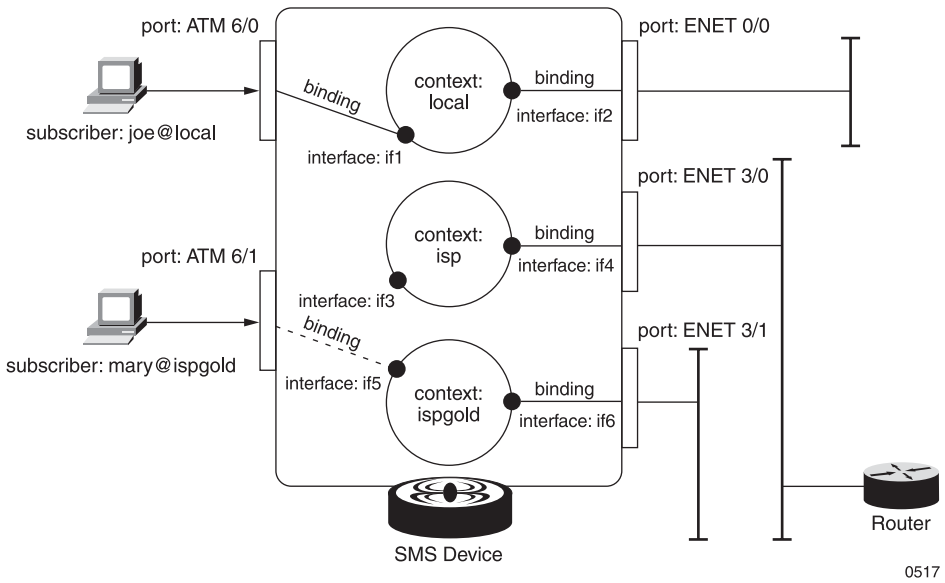
Figure 1-2 AOS Application



AOS Concepts

Figure 1-3 illustrates the relationships between different AOS software components. The rest of this section describes these components in greater detail.

Figure 1-3 AOS Software Component Interrelationships



Contexts

Most networking products are designed so that the entire set of ports, circuits, and protocols operate together as one global instance. The AOS supports an advanced feature called multiple contexts. Each AOS context is a virtual SMS device running within a single physical device. A context has its own IP routing table, its own Remote Authentication Dial-In User Service (RADIUS) client, and so on, and does not share this information with other contexts. By separating the address and name spaces in this way, service providers can use multiple contexts to manage subscribers and provide access for customers of different providers, or to provide different classes of services for customers. Service providers can use a single physical device to implement this, with one or more contexts being assigned to each service provider or service class.

Figure 1-3 shows three contexts configured within a single Redback device: local, isp, and ispgold. The contexts `isp` and `ispgold` illustrate the use of multiple contexts to provide different classes of service. For example, context `isp` can provide a standard level of service, while context `ispgold` can support a premium level of service, such as higher-speed access. Each of the three contexts functions independently of the others.

An SMS device with a single context configured is similar to traditional networking products. This is referred to as a single-context configuration.

Every configuration includes a special context named local that cannot be deleted. In single-context configurations, this is the only context. The local context allows you to do the following:

- Configure and examine other contexts.
- Configure global resources such as ports, the Simple Network Management Protocol (SNMP), and system logging.

Each context provides a separate security, management, and operating environment on behalf of a given network. You configure interface and subscriber information as part of a context.

Interfaces

The concept of an interface in the AOS differs from that in traditional networking devices. The term, interface, is often used synonymously with port or circuit, which are physical entities. In the AOS, an interface is a logical construct that provides higher-layer protocol and service information, such as layer 3 addressing. Interfaces are configured as part of a context, and are independent of physical ports and circuits. The decoupling of the interface from the physical layer entities enables many of the advanced features offered by the AOS.

For the higher-layer protocols to become active, you must associate an interface with a physical port or circuit. This association is referred to as a binding in the AOS.

In Figure 1-3, each context shows two interfaces. These interfaces are configured within each context. The bindings shown in the figure are not present when the interfaces are configured; they are configured later.

Subscribers

Subscribers are the endusers of the high-speed access services. You configure subscriber records as part of a context, either locally on the SMS device or on a RADIUS server. Subscriber records contain the information necessary to bind a subscriber to the correct interface, and therefore, to the correct network context and services. Subscriber records can also contain other configuration information, such as authentication, access control, rate-limiting, and policing information.

Ports and Circuits

Ports and circuits in the AOS represent the physical connectors and channels on the SMS hardware I/O modules. Physical port and circuit configuration includes traffic profiles and data encapsulation information. Traffic profiles provide a configuration shortcut. A single traffic profile with traffic shaping, counter, and statistics configuration information can be applied to multiple ports. All circuits must have a configured encapsulation.

For configuration purposes, Ethernet ports are treated as a single circuit. This means that many of the generic circuit configuration commands are also available in Ethernet port configuration mode.

Before any higher-layer user data can flow through a physical port or circuit, you must associate that port or circuit with an interface, a bypass, or a tunnel within a context. This association is referred to as a binding in the AOS. The configuration for each port and circuit includes binding information.

Bindings

Bindings form the association in the AOS between the circuits or tunnels and the higher-layer bridging, routing, and switching protocols configured for a given context. No user data can flow on a circuit or Ethernet port until some higher-layer service is configured and associated with it. Bindings are either statically mapped during configuration or dynamically created based on subscriber characteristics as defined in the local database, or on a RADIUS server. Once bound, traffic flows through the context as it would through any IP router.

Static binding occurs when you bind a circuit directly to an interface. In this case, the circuit is hard-wired to the higher-layer protocols defined for the interface. This is the simplest form of binding available in the AOS, providing functionality similar to that provided by traditional network devices, such as routers. You can use static bindings for any circuit with any encapsulation type. The bindings between the Ethernet ports and the interfaces within the contexts shown in Figure 1-3 are static bindings.

You can also statically bind a circuit to a particular subscriber in a given context. In this case, the binding between the circuit and the higher-layer protocols is determined indirectly, through the subscriber record. In Figure 1-3, subscriber `joe` is configured with an IP address that maps to interface if1 in context local. When the virtual circuit on Asynchronous Transfer Mode (ATM) port 6/0 is bound to subscriber `joe`, the AOS determines the interface that the circuit will be bound to by looking at the subscriber information for `joe`.

Dynamic binding occurs when you bind a circuit to the higher-layer protocols based on session information. For example, a Point-to-Point Protocol (PPP) encapsulated session may be bound to a particular context and interface by examining the authenticated structured username in the form: user@context.

Dynamic binding is the key to enabling advanced features such as dynamic service and provider selection. Dynamic binding also enables simultaneous access to multiple services on a single circuit.

Figure 1-3 shows a dynamic binding between the virtual channel on ATM port `6/1` and interface `if5` in context `ispgold`. When the subscriber initiates a PPP session using the structured username `mary@ispgold`, the AOS determines the context (`ispgold`) for the connection, and selects an interface (`if5`) to bind the circuit to. Successful dynamic binding depends on subscriber information for `mary` configured in context `ispgold`, and successful PPP authentication during PPP session establishment. The binding between this circuit and the ispgold context will be removed when the PPP session is terminated. Because the binding on the circuit is dynamic, this same circuit could be used by a different subscriber to select a different service.

User Interface Commands

This chapter describes the commands you use to begin and end command line sessions and to access the operator (nonprivileged) exec and administrator (privileged) exec command modes. The command-line interface (CLI) only requires you to enter enough of any command or keyword to uniquely identify it.

For a general overview of the CLI, see the "Understanding the User Interface" chapter in the *Access Operating System (AOS) Configuration Guide*.

? (help)

? (help)

Purpose

Displays brief system help on the available commands or command options.

Command Mode

This command can be used in any mode.

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **?** command to display brief system help on the available command or command options.

To list all valid commands available in the current mode, enter a question mark (**?**) at the system prompt.

To list the associated keywords or arguments for a command, enter a question mark (**?**) in place of a keyword or argument on the command line. This form of help is called command syntax help, because it lists the keywords or arguments that apply to the command based on the command, keywords, and arguments you have already entered.

To obtain a list of commands or keywords that begin with a particular character string, enter the abbreviated command or keyword immediately followed by a question mark (**?**). This form of help is called word help, because it lists only the commands or keywords that begin with the abbreviation you entered.

Examples

The following example shows how to display the commands available in operator exec mode:

```
[local]RedBack>?

  atm         ATM commands
  bulkstats   Manage bulk statistics collection file
  clear       Clear information
  default     Return an option to it's default value
  enable      Modify command mode privilege
  exit        Exit exec mode
```

```
  no          Disable an interactive option
  ping        Packet Internet Groper Command
  show        Show running system information
  terminal    Modify terminal settings
  traceroute  Trace route to destination
```

The following example shows how to use command syntax help to display the next argument of a partially complete static route command:

```
[local]RedBack(config-ctx)#ip route ?

  A.B.C.D  destination IP address to be statically configured
[local]RedBack(config-ctx)#ip route
```

Related Commands

None

enable

enable [*level*]

no enable

Purpose

Modifies the privilege level for the current exec session.

Command Mode

operator exec

Syntax Description

level	Optional. Requested privilege level. The range of values is 0 to 15; the default is 15.

Default

An exec session runs at the starting privilege level for the administrator.

Usage Guidelines

Use the **enable** command to modify the privilege level for the current exec session.

Valid administrator usernames and passwords must be configured for the appropriate context. If no administrators are configured, privileged mode can be accessed only from the console.

Use the *level* argument to select the desired privilege level, up to the maximum privilege level configured for this operator or administrator account. If this argument is omitted, the maximum privilege level (15) is enabled.

Use the **no** form of this command to return to the starting privilege level configured for this operator or administrator account.

Examples

The following example shows a user entering the **enable** command during a Telnet session. The user is prompted to enter a password, which is not displayed on the screen. After the user enters the correct password, the system enters administrator mode as indicated by the pound sign (#) in the prompt.

```
[local]RedBack>enable

Password:
[local]RedBack#
```

Related Commands

administrator
exit
operator
privilege max
privilege start
show privilege

end

end

Purpose

Exits the current configuration mode and returns to administrator exec mode.

Command Mode

This command can be used in all configuration modes.

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **end** command to exit the current configuration mode and return to administrator exec mode.

Examples

The following example shows an administrator exiting interface configuration mode and returning to administrator exec mode:

```
[local]RedBack(config-if)#end
[local]RedBack#
```

Related Commands

configure
exit

exit

exit

Purpose

Exits the current configuration mode and returns to the next highest level configuration mode. At the exec prompt, closes an active terminal or console session, and terminates the exec.

Command Mode

This command can be used in any mode.

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **exit** command to exit the current configuration mode, return to operator exec mode, or close an active terminal or console session. Entering this command in any configuration mode exits the current configuration mode and returns to the next highest level configuration mode. Entering this command in administrator exec mode returns to operator exec mode. Entering this command in operator exec mode closes an active terminal or console session, and terminates the exec.

Examples

The following example shows an administrator exiting interface configuration mode and returning to context configuration mode:

```
[local]RedBack(config-if)#exit
[local]RedBack(config-ctx)#
```

The following example shows how to exit an active Telnet session:

```
[local]RedBack>exit
```

Related Commands

configure
end

show privilege

show privilege

Purpose

Displays the current privilege level for the exec session.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show privilege** command to display the current privilege level for the exec session.

Examples

The following command displays sample output from the **show privilege** command:

```
[local]RedBack#show privilege

The current privilege level is 15
```

Related Commands

enable
privilege max
privilege start

Terminal Settings and Telnet Commands

This chapter contains descriptions for commands used to configure terminal settings, to configure AOS for remote access through Telnet and Secure Shell (SSH), and to access remote systems using Telnet supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure terminal settings and Telnet, and configuration examples, see the "Accessing the AOS" chapter in the *Access Operating System (AOS) Configuration Guide*.

administrator reserve

administrator reserve {**ipaddress** *ip-address* | **name** *admin-name*} **context** c*tx-name* **sessions** *sessions*

no administrator reserve {**ipaddress** *ip-address* | **name** *admin-name*} **context** *ctx-name* **sessions** *sessions*

Purpose

Reserves remote sessions for a particular IP address or username.

Command Mode

global configuration

Syntax Description

ipaddress *ip-address*	IP address for which to reserve the remote sessions.
name *username*	Username of the operator or administrator for which to reserve the remote sessions. The *username* argument must be specified in the format *username@ctx-name*.
context *ctx-name*	Context in which the IP address is defined.
sessions *sessions*	Number of sessions to be reserved. The range of values is 1 to 8.

Default

No sessions are reserved.

Usage Guidelines

Use the **administrator reserve** command to reserve remote sessions for a particular IP address or username. This guarantees that the specified number of remote sessions are available for use by the specified IP address or username for Telnet, Secure Shell (SSH), or HTTP access to the system. If the sessions are not available at the time that the command is issued, the command displays a message and does not reserve any sessions.

Use the **no** form of this command to release the reserved remote sessions.

Examples

The following example reserves two remote sessions for IP address `192.168.190.32` in the `local` context:

```
[local]RedBack(config)#administrator reserve ipaddress 192.168.190.32 context local
sessions 2
```

The following example reserves four remote sessions for the administrator `superuser` in the `local` context:

```
[local]RedBack(config)#administrator reserve name superuser context local sessions 4
```

Related Commands

show administrator reservations

clear tty

clear tty *num*

Purpose

Ends a remote (Telnet or Secure Shell [SSH]) session for an administrator or an operator.

Command Mode

operator exec

Syntax Description

num	Session number as shown in the **show administrators** command. The range of values is 1 to 8.

Default

None

Usage Guidelines

Use the **clear tty** command to end a remote session on the system. An operator in the local context can end any administrator session. Operators in any other context can only end sessions in their own context.

Examples

The following command clears session number 3:

```
[local]RedBack>clear tty 3
```

Related Commands

clear subscriber
show administrators

console-break-enable

console-break-enable

no console-break-enable

Purpose

On the Subscriber Management System (SMS) 10000, enables dump output to the console. On all other SMS devices, enables the use of the **Break** key to reload the system.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

On the SMS 10000, system dump information is not printed to the console. On all other SMS devices, the **Break** key cannot be used to reload the system.

Usage Guidelines

Use the **console-break-enable** command to enable the display of system dump information on the console for an SMS 10000 device; use this command to enable the use of the **Break** key to reload the system for all other SMS devices.

Use the **no** form of this command to disable the printing of dump information on the SMS console for an SMS 10000, or to disable the use of the **Break** key to reload the system on all other SMS devices.

Examples

The following command enables the use of the **Break** key to reload the system:

```
[local]RedBack(config)#console-break-enable
```

Related Commands

reload

debug ip telnet

debug ip telnet

no debug ip telnet

Purpose

Enables the logging of Telnet debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip telnet** command to log all Telnet debugging messages. You can use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example turns on debug logging for all Telnet sessions:

```
[local]RedBack#debug ip telnet
```

Related Commands

logging console
show cm stats
telnet
terminal monitor

debug sshd

debug sshd [*debug-level*]

no debug sshd

Purpose

Enables the logging of Secure Shell (SSH) debugging messages on the system.

Command Mode

administrator exec

Syntax Description

debug-level	Optional. Level of debugging. The range of values is 0 (minimal debugging) to 10 (maximum debugging); the default value is 5.

Default

SSH debugging is disabled.

Usage Guidelines

Use the **debug sshd** command to enable the logging of SSH debug messages on the system. You can use the **logging console** or **terminal monitor** commands to display the messages in real time.

Use the **no** form of this command to disable SSH debugging.

Examples

The following example enables SSH debugging with a debug level of 8:

```
[local]RedBack#debug sshd 8
```

Related Commands

logging console
terminal length
terminal monitor
terminal width

length

length *length*

default length

Purpose

Sets the initial terminal length for the console or terminal when a user logs on to the system.

Command Mode

line configuration

Syntax Description

length	Number of lines of the terminal displays. Allowable values are 0 and any number in the range 5 to 4,294,967,295; the default is 24.

Default

The default terminal length is 24 lines.

Usage Guidelines

Use the **length** command to set the length to which the terminal is initialized when a user logs on to the Access Operating System (AOS). You can override this setting for any session by entering administrator exec mode and using the **terminal length** command.

If you set the terminal length to 0, auto-more processing is disabled (see the "Understanding the User Interface" chapter in the *Access Operating System (AOS) Configuration Guide*).

Note Changing the line length for a line that currently has a user logged in does not affect that user's settings, only the settings that the user sees at the next logon.

Use the **default** form of this command to return the terminal length to 24 lines.

Examples

The following example sets the console length to 48 lines:

```
[local]RedBack(config)#line console
[local]RedBack(config-line)#length 48
```

Related Commands

terminal length
terminal width
width

line

line {**console** | **tty** *start-tty* [**through** *end-tty*]}

Purpose

Enters line configuration mode to configure default terminal settings.

Command Mode

global configuration

Syntax Description

console	Specifies the console terminal line.
tty *start-tty*	Number of the remote session terminal line (or the starting number if specifying a range). The range of values is 0 to 8.
through *end-tty*	Optional. Last line number in a range of remote session terminal lines.

Default

The terminal length is 24 lines and the terminal width is 80 characters for all console and remote sessions.

Usage Guidelines

Use the **line** command to enter the line configuration mode, so that you can set the length and width of the console or one or more sessions.

Examples

The following example enters line configuration mode for the console terminal line:

```
[local]RedBack(config)#line console
[local]RedBack(config-line)#
```

Related Commands

length
width

show administrator reservations

show administrator reservations

Purpose

Displays information on remote session reservations.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show administrator reservations** command to display information related to remote (Telnet and Secure Shell [SSH]) session reservations on the system.

Examples

The following example shows remote session reservation information:

```
[local]RedBack>show administrator reservations

 session 1: client 192.168.12.35 active not reserved
 session 2: client 192.168.12.35 active not reserved
 session 3: inactive reserved for 192.168.190.32
 session 4: inactive reserved for 192.168.190.32
 session 5: inactive reserved for 192.168.190.32
 session 6: inactive reserved for 192.168.190.32
 session 7: inactive not reserved
 session 8: inactive not reserved
```

Related Commands

administrator reserve

show terminal

show terminal [*terminal-number*]

Purpose

Displays the terminal length and width settings for a terminal session.

Command Mode

operator exec

Syntax Description

terminal-number	Optional. Number of the terminal for which the setting information is preferred. The range of values is 0 to 8.

Default

Displays the terminal length and width settings for the current terminal session.

Usage Guidelines

Use the **show terminal** command to display the terminal settings for a session. You can identify the terminal number of a specific session by using the **show administrators** command in operator exec mode. Omit the *terminal-number* argument to display information for the current session.

Examples

The following example shows the settings for terminal number `0` (the console):

```
[local]RedBack>show terminal 0

Terminal 0: length 24, width 80.
```

Related Commands

show administrators
terminal length
terminal width

sshd keygen

sshd keygen

Purpose

Generates a new Secure Shell (SSH) key and enables SSH on the system.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

SSH is disabled.

Usage Guidelines

Use the **sshd keygen** command to generate a new SSH key (or replace an existing key) and enable SSH on the system. The key is stored in the file named /flash/sshd.key. If a key already exists, the existing key is replaced.

This command does not have a **no** or **default** form. To remove the key and disable SSH, use the **delete** command in administrator exec mode to remove the key file.

Examples

The following example enables SSH on the system:

```
[local]RedBack#sshd keygen
```

The following example removes the SSH key file and disables SSH:

```
[local]RedBack#delete /flash/sshd.key
```

Related Commands

debug sshd
delete

telnet

telnet {*ip-address* | *hostname*} [*port*]

Purpose

Establishes a Telnet session from the Subscriber Management System (SMS) device to a host.

Command Mode

administrator exec

Syntax Description

ip-address	IP address of the host with which to establish the Telnet session.
hostname	Hostname of the host with which to establish the Telnet session. The Domain Name System (DNS) must be enabled to use the *hostname* argument.
port	Optional. User Datagram Protocol (UDP) port used to communicate with the host. The range of values is 1,025 to 10,000; the default is 23.

Default

None

Usage Guidelines

Use the **telnet** command to establish a Telnet session from the SMS device to a host. The *hostname* argument can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, "DNS Commands."

Use the *port* argument to specify a port other than the default UDP port. Ensure that the port on the remote host is activated for Telnet.

Examples

The following example establishes a Telnet session with a host at IP address `192.168.190.32`:

```
[local]RedBack#telnet 192.168.190.32
```

The following example establishes a Telnet session to a host at IP address `192.168.190.32` via port `2222`:

```
[local]RedBack#telnet 192.168.190.32 2222
```

Related Commands

ip domain-lookup
ip domain-name
ip name-servers

terminal length

terminal length *length*

default terminal length

Purpose

Sets the terminal length to be used for the administrator or operator's terminal for the duration of the current exec session.

Command Mode

operator exec

Syntax Description

length	Number of lines to be used for the terminal length. The range of values is 0 and 5 to 4,294,967,295; the default is 24.

Default

The default terminal length is 24 lines.

Usage Guidelines

Use the **terminal length** command to set the length in terminal lines for an exec session. Upon exit of the exec session, the value is reset to the default length of 24 lines. Setting the terminal length to 0 disables auto-more processing.

Use the **default** form of this command to return the terminal length to the default value.

Examples

The following command sets the session terminal length to `30` lines:

```
[local]RedBack>terminal length 30
```

Related Commands

show terminal
terminal width

terminal monitor

terminal monitor [**circuit** {*slot/port* [*vpi vci* | [**hdlc-channel** *name*] *dlci* | **lac** *vcn* | **lns** *vcn* | **pppoe** [*cm-slot-*]*session-id* [**cm** *slot*]} [**only**]]

no terminal monitor [**circuit** {*slot/port* [*vpi vci* | [**hdlc-channel** *name*] *dlci*] | **lac** *vcn* | **lns** *vcn* | **pppoe** [*cm-slot-*]*session-id* [**cm** *slot*]} [**only**]]

Purpose

Displays system events on a remote (Telnet or Secure Shell [SSH]) session continuously as they are logged.

Command Mode

operator exec

Syntax Description

circuit	Optional. Selects events for a specific circuit.
slot/port	Backplane slot number and port number of the port for which circuits are displayed.
vpi	Virtual path identifier (VPI) for an Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC). The range of values is 0 to 255.
vci	Virtual channel identifier (VCI) for an ATM PVC. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
hdlc-channel *name*	Optional. Name of the High-Level Data Link Control (HDLC) channel. Specified only for channelized DS-3 ports only.
dlci	Data- link connection identifier (DLCI). Specified for Frame Relay ports only. The range of values is 16 to 991.
lac *vcn*	Virtual circuit number (VCN) for Layer 2 Tunneling Protocol Access Controllers (LACs). The range of values is 0 to 65,534.
lns *vcn*	Virtual circuit number (VCN) for Layer 2 Tunneling Protocol Network Services (LNSs). The range of values is 0 to 65,534.
pppoe [*cm-slot-*]*session-id*	Point-to-Point Protocol over Ethernet (PPPoE) session identifier. The *cm-slot* argument is required for Connection Manager (CM) modules and not used in any other case. It specifies the CM slot number. The session ID must be entered for all platforms. The range of values is 1 to 65,534.
cm *slot*	Slot number of the CM module for the session. Specified only for hardware platforms that support CM modules.

only	Optional. Specifies that messages with no circuit association are not displayed.

Default

Events are not logged to administrator terminals.

Usage Guidelines

Use the **terminal monitor** command to enable logging of events to the current terminal. This command can be useful for seeing the Event Log output while connected to a system by Telnet or Secure Shell (SSH), rather than working on the console. This command is not valid on the console terminal. If you want to enable logging to the console terminal, use the **logging console** command in global configuration mode.

Use the **circuit** keyword to narrow the events viewed to a specific circuit. All messages that are associated with the defined circuit specification and messages that have no circuit association are displayed on the remote session. You can use the **only** keyword to filter out messages with no circuit association.

Note You can only use the **circuit** keyword with ATM, Frame Relay, and Ethernet ports with PPPoE encapsulation.

Use the **no** form of this command to disable terminal monitoring.

Examples

The following example enables event logging to a Telnet connection:

```
[local]RedBack>terminal monitor
```

The operator or administrator can narrow the messages displayed to those pertaining to a specific circuit (VPI:VCI `4:200` on ATM slot `3`, port `1`) with the following command:

```
[local]RedBack>terminal monitor circuit 3/1 4 200 only
```

Related Commands

logging console
logging filter
logging syslog
show log
show logging

terminal width

terminal width *width*

default terminal width

Purpose

Sets the terminal width in characters to be used for the administrator or operator's terminal for the duration of the current exec session.

Command Mode

operator exec

Syntax Description

width	Preferred terminal width setting in characters. The range of values is 5 to 512; the default is 80.

Default

The default terminal width is 80 characters.

Usage Guidelines

Use the **terminal width** command to set the width in characters of the terminal for an exec session. Upon exit from the this session, the value is reset to the default width of 80 characters.

Use the **default** form of this command to change the terminal width back to the default value.

Examples

The following command changes the session terminal width to `70` characters:

```
[local]RedBack>terminal width 70
```

Related Commands

show terminal
terminal length
width

width

width *width*

default width

Purpose

Sets the initial terminal width for the console or terminal when a user logs on to the system.

Command Mode

line configuration

Syntax Description

width	Number of characters the terminal displays on a line. The range of values is 5 to 512; the default is 80.

Default

The default value is 80 columns.

Usage Guidelines

Use the **width** command to set the initial terminal width when the user logs on to the Access Operating System (AOS). You can override this setting for any session by using the **terminal width** command.

Note Changing the line width for a line that currently has a user logged in does not affect that user's settings, only the settings that the user sees at the next logon.

Use the **default** form of this command to return the initial terminal width for this line to the default value of 80 columns.

Examples

The following example sets the initial terminal width for all console sessions to `70` columns:

```
[local]RedBack(config)#line console
[local]RedBack(config-line)#width 70
```

Related Commands

length
show terminal
terminal width

System Image and Configuration File Commands

This chapter provides descriptions for the commands that are used to manage system image and configuration files supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to manage system image and configuration files, and configuration examples, see the “System Images and Configuration Files” chapter in the *Access Operating System (AOS) Configuration Guide*.

boot configuration

boot configuration *url*

no boot configuration *url*

default boot configuration

Purpose

Specifies a configuration file to be read when the system boots.

Command Mode

global configuration

Syntax Description

url	Name of the configuration file to be read at boot time.

Default

For systems with a /flash device, the boot configuration file is /flash/redback.cfg. For systems with no /flash device, the boot configuration file is /pcmcia0/redback.cfg.

Usage Guidelines

Use the **boot configuration** command to specify the configuration file to be read when the system boots. You can execute this command multiple times to specify several boot configuration files. The Access Operating System (AOS) reads each file successively until all the files and the commands they contain are executed into the system's configuration. While individual commands within a file might fail (for instance, if a syntax error is encountered), there is no notion of a configuration file itself passing or failing. You can add comments to a configuration file by beginning a line with the **#** character; the AOS does not process comment lines.

You must specify a file on the local file system, with a URL in the following form:

[**file:**][**/sm**]*/device*[*/directory*]*/filename.ext*

The **/sm** keyword applies only to systems that are configured with redundant System Manager (SM) modules. You can only specify a boot configuration file on the active SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Use the **no** form of this command to undo a previous **boot configuration** command. You must provide the same *url* argument provided in that previous command. If all **boot configuration** commands are subsequently undone by corresponding **no boot configuration** commands, then no configuration occurs upon system boot.

Use the **default** form of this command to set the configuration file to the default boot configuration file, as specified earlier. Any other boot configuration files previously specified are removed.

Examples

The following example instructs the system to configure itself from the file named `old_config.cfg`:

```
[local]RedBack(config)#boot configuration /flash/old_config.cfg
```

The following example first undoes the effect of the example immediately above, then instructs the system to configure itself by reading both `redback.cfg` and then `additional.cfg`:

```
[local]RedBack(config)#no boot configuration /flash/old_config.cfg
[local]RedBack(config)#boot configuration /flash/redback.cfg
[local]RedBack(config)#boot configuration /flash/additional.cfg
```

The following example resets the configuration file to be the default:

```
[local]RedBack(config)#default boot configuration
```

Related Commands

boot system
configure
reload

boot system

boot system {**bootp** | *url* **local** *local-ipaddr* [**gateway** *gw-ipaddr*]}

no boot system {**bootp** | *url* **local** *local-ipaddr* [**gateway** *gw-ipaddr*]}

default boot system

Purpose

Specifies the location of a system image to use at the next system boot.

Command Mode

global configuration

Syntax Description

bootp	Specifies that the system be booted from an image configured on a Bootstrap Protocol (BOOTP) server.
url	URL of the image to be used in the next system boot.
local *local-ipaddr*	IP address to be used by the system's boot loader in communicating with a Trivial File Transfer Protocol (TFTP) server, in the form A.B.C.D. This argument must be specified for, and is only valid for TFTP files.
gateway *gw-ipaddr*	Optional. IP address of a default router to be used by the system's boot loader in communicating with a TFTP server, in the form A.B.C.D. This argument must be specified for, and is only valid for TFTP files.

Default

For systems with a /flash device, the system image file is /flash/redback.bin. For systems with no /flash device, the system image file is /pcmcia0/redback.bin.

Usage Guidelines

Use the **boot system** command to specify the location of a system image to use at the next system boot. You can issue this command multiple times to specify a list of image files to try. The Access Operating System (AOS) attempts to load the images, in the order specified, until an image is successfully loaded.

When referring to a file on a TFTP server, the URL takes the following form, where the *ip-address* argument is the IP address, or the *hostname* argument is the hostname of the TFTP server. The specified host must be reachable through the active Ethernet management port.

tftp://{*ip-address* | *hostname*}[/*directory*]/*filename.ext*

When referring to a file on an FTP server, the URL takes the following form, where the *username:passwd* argument specifies the user and an optional password, the *ip-address* argument is the IP address of the FTP server, and the *hostname* argument is the hostname of the FTP server. The **passive** keyword specifies a passive FTP transaction.

ftp://*username*:*passwd*@{*ip-address* | *hostname*}[/*directory*]/*filename.ext* **passive**

The *hostname* argument for TFTP or FTP can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, "DNS Commands."

When referring to a file on the local file system, the URL takes the following form:

[**file:**][**/sm**]/*device*[/*directory*]/*filename.ext*

The **/sm** specification applies only to systems that are configured with redundant System Manager (SM) modules. You can only specify an image file on the active SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Use the **no** form of this command to undo a previous **boot system** command. You must provide the same *url* argument provided in that previous command. If all **boot system** commands are subsequently undone by corresponding **no boot system** commands, the net effect is as if the **default boot system** command had been entered; that is, there is no way to specify that the system does not boot at all.

Use the **default** form of this command to set the system image file to the default, as specified above. Any other boot system files previously specified are removed.

Examples

The following example sets up the boot loader to attempt to boot from a BOOTP server and, if that fails, to try a locally stored file named `fallback.bin`:

```
[local]RedBack(config)#boot system bootp
[local]RedBack(config)#boot system /flash/fallback.bin
```

The following example resets the boot loader to use the default file:

```
[local]RedBack(config)#default boot system
```

Related Commands

boot configuration
configure
ip domain-lookup
ip domain-name
ip name-servers
reload

configure

configure [*url* [**verbose**]]

Purpose

Enters global configuration mode or configures the system from a preexisting configuration file.

Command Mode

administrator exec

Syntax Description

url	Optional. URL of a preexisting configuration file.
verbose	Optional. Displays each line and its line number when configuring from a preexisting configuration file.

Default

Enters global configuration mode.

Usage Guidelines

Use the **configure** command to enter global configuration mode or to configure the system from a configuration file. If the *url* argument is not specified, the system enters global configuration mode. If the *url* argument is specified, configuration commands are read from the associated file.

When referring to a file on the local file system, the URL takes the following form:

[**file:**][**/sm**]*/device*[*/directory*]*/filename.ext*

The **/sm** specification applies only to systems that are configured with redundant System Manager (SM) modules. You can only specify an image file on the active SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

When referring to a file on a Trivial File Transfer Protocol (TFTP) server, the URL takes the following form, where the *ip-address* argument is the IP address, or the *hostname* argument is the hostname of the TFTP server:

tftp://{*ip-address* | *hostname*}[*/directory*]*/filename.ext*

The *hostname* argument for TFTP or FTP can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, “DNS Commands.”

After you enter the **configure** command, the system prompt changes from [*context*]*hostname*# to [*context*]*hostname* (config)#, where *hostname* is the local hostname, indicating that you are in global configuration mode. To leave global configuration mode and return to the administrator exec prompt, use the **end** command.

Examples

The following example enters global configuration mode:

```
[local]RedBack#configure

Enter configuration commands, one per line, 'end' to exit
[local]RedBack(config)#
```

The following example configures the system from a configuration file on the local file system:

```
[local]RedBack#configure /flash/old_config.cfg
```

Related Commands

copy
directory
exit
ip domain-lookup
ip domain-name
ip name-servers
show configuration

copy

copy *url1 url2* [**passive**] [**-noconfirm**]

Purpose

Copies files from either a Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) server to the Subscriber Management System (SMS) device; from the SMS device to a TFTP or FTP server; or from one location to another on the local SMS file system.

Command Mode

administrator exec

Syntax Description

url1	URL of the file that is to be copied.
url2	URL of the destination of the copy operation.
passive	Optional. Specifies the use of passive mode FTP.
-noconfirm	Optional. Avoids a confirmation prompt when overwriting an existing file on the local file system.

Default

None

Usage Guidelines

Use the **copy** command to copy files to or from an SMS device. At least one of the files, either the source or destination file, must be on a local file system. When referring to a file on the local file system, the URL takes the following form:

[**file:**][*/sm*]*/device*[*/directory*]*/filename.ext]*

The */sm* argument is used only for systems that are configured with redundant System Manager (SM) modules. You can specify files on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the */sm* argument in the destination URL to specify a device on both the active and backup SM module. Omit the */sm* argument in the source URL to specify the active SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Note On a system that is configured with redundant SM modules, you can also use the **copy** command to copy the entire contents of a device on the active SM module to a device on the backup SM module, or from the backup SM module to the active SM module. To do this, include the appropriate */sm* argument and the device in both the source file and destination file URLs. You cannot copy files from the backup SM module to the active SM module.

When referring to a file on a TFTP server, the URL takes the following form, where the *ip-address* argument is the IP address, or the *hostname* argument is the hostname of the TFTP server:

tftp://{*ip-address* | *hostname*}[/*directory*]/*filename.ext*

When referring to a file on an FTP server, the URL takes the following form, where the *username:passwd* argument specifies the user and an optional password, the *ip-address* argument is the IP address of the FTP server, and the *hostname* argument is the hostname of the FTP server. The **passive** keyword specifies a passive FTP transaction.

ftp://*username*:*passwd*@{*ip-address* | *hostname*}[/*directory*]/*filename.ext* **passive**

The *hostname* argument for TFTP or FTP can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, "DNS Commands."

Note When you use the **copy** command on a synchronous RAM (SRAM) card that is formatted for Dynamic Host Configuration Protocol (DHCP) secured Address Resolution Protocol (ARP), an error message is displayed and the command is not carried out. The message says that the device is `formatted for dhcp-secured-arp`.

Examples

The following example copies a file from the TFTP server to the local file system. If the file already exists, you get a prompt asking if you want to overwrite the existing file.

```
[local]RedBack#copy tftp://192.168.3.141/aos.cfg /flash/aos.cfg
```

The following example copies a file from one location to another of the local file system:

```
[local]RedBack#copy /flash/redback.bin /flash/backup/redback.bin
```

The following example copies a file from the FTP server with an IP address of `192.168.145.99` to `/flash`:

```
[local]RedBack#copy ftp://john:test@192.168.145.99/redback.cfg /flash/
```

The following example performs the same operation described in the preceding example applies, except that the FTP operation is passive:

```
[local]RedBack#copy ftp://john:test@192.168.145.99/redback.cfg /flash/ passive
```

The following command copies all the files on pcmcia0 on the active SM module (SM2) to pcmcia0 on the backup SM module (SM3):

```
[local]RedBack#copy /sm2/pcmcia0 /sm3/pcmcia0
```

Related Commands

delete
directory
ip domain-lookup
ip domain-name
ip name-servers
rename

debug ip tftp

debug ip tftp

no debug ip tftp

Purpose

Enables the logging of Trivial File Transfer Protocol (TFTP) debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip tftp** command to enable the logging of TFTP debugging messages. You can use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely effect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example turns on debug logging for TFTP processes:

```
[local]RedBack#debug ip tftp
```

Related Commands

copy
logging console
show cm stats
terminal monitor

delete

delete *url* [**-noconfirm**]

Purpose

Deletes a file on the local file system.

Command Mode

administrator exec

Syntax Description

url	Identification of a preexisting file on a local file system.
-noconfirm	Optional. Deletes special files without asking for confirmation.

Default

None

Usage Guidelines

Use the **delete** command to remove a file from the local file system. When referencing a file, a full path name of the following form is required:

[**file:**][*/sm*]*/device*[*/directory*]/*filename.ext*

The */sm* argument is used only for systems that are configured with redundant System Manager (SM) modules. You can specify files on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the */sm* argument to specify a device on both the active and backup SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Use the **-noconfirm** keyword when deleting the special files redback.bin and redback.cfg. The **delete** command without the **-noconfirm** keyword seeks confirmation when the user attempts to delete the redback.bin or redback.cfg files.

Note When you use the **delete** command on a synchronous RAM (SRAM) card that is formatted for Dynamic Host Configuration Protocol (DHCP) secured Address Resolution Protocol (ARP), an error message is displayed and the command is not carried out. The message says that the device is `formatted for dhcp-secured-arp`.

Examples

The following example deletes a file in a nested subdirectory:

```
[local]RedBack#delete /flash/backup/97dec/aos.cfg
```

Related Commands

copy
directory
rename

directory

directory *url* [**-size** | **-time**] [**-reverse**]

Purpose

Displays a list of files on a local file system.

Command Mode

administrator exec

Syntax Description

url	Identification of the device, and optionally the subdirectory, for which files are displayed.
-size	Optional. Specifies that the files are displayed in order of size, starting with the smallest.
-time	Optional. Specifies that the files are displayed in order of time, starting with the oldest.
-reverse	Optional. Specifies that files are displayed in reverse order.

Default

Files are displayed in alphabetical order.

Usage Guidelines

Use the **directory** command to display a list of files on the local file system. When referencing a directory path, you must use the following form:

[*/sm*]*/device*[*/path*]

The */sm* argument is used only for systems that are configured with redundant System Manager (SM) modules. You can specify files on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the */sm* argument to specify the active SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Note When you use the **directory** command on a synchronous RAM (SRAM) card that is formatted for Dynamic Host Configuration Protocol (DHCP) secured Address Resolution Protocol (ARP), an error message is displayed and the command is not carried out. The message says that the device is `formatted for dhcp-secured-arp`.

Examples

The following example displays a list of files in the root directory of the flash file system:

```
[local]RedBack#dir /flash

  size          date       time       name
--------       ------     ------    --------
     512    APR-10-2001  10:50:40   CONFIG           <DIR>
     327    APR-07-2001  15:02:42   REDBACK.BAK
 4836696    DEC-02-2000  16:18:42   REDBACK.BIN
     726    JUN-19-2001  10:58:48   REDBACK.CFG

total bytes: 6946816, used bytes:4876288, free bytes: 2070528
```

The following example displays a list of files in a subdirectory of the flash file system, listed in reversed time order (newest first):

```
[local]RedBack#dir /flash/config -time -reverse

  size          date       time       name
--------       ------     ------    --------
     902    AUG-23-2000  08:49:10   RBAK.CFG
     726    AUG-23-2000  08:48:54   TEST.CFG
     512    APR-10-2001  10:50:40   ..               <DIR>
     512    APR-10-2001  10:50:40   .                <DIR>

total bytes: 6946816, used bytes:4876288, free bytes: 2070528
```

Related Commands

copy
mkdir
rename
rmdir

fabric revert

fabric revert

no fabric revert

Description

Specifies that the system should automatically revert to the default fabric modules when the modules become available.

Command Modes

administrator exec
global configuration

Syntax Description

This command has no keywords or arguments.

Default

The fabric modules are nonreverting.

Usage Guidelines

Use the **fabric revert** command to specify that the system should always use the default fabric modules, when they are available.

This command applies only to the Subscriber Management System (SMS) 10000 hardware platform. The SMS 10000 device can be configured with up to four fabric modules: A, B, C, and D. Under normal operating conditions, the system uses the default fabric modules A, B, and C. If fabric module D is installed in the system, it is standby. In the case that one of the default fabric modules fails, fabric D is used. The **fabric revert** command is used to instruct the system what to do if a failed fabric module becomes available (for example, is replaced).

In global configuration mode, this command instructs the system to automatically revert to fabric modules A, B, and C, when these modules are available.

Use the **no** form of this command in global configuration mode to configure the system so that it does not automatically revert to fabric modules A, B, and C when these modules are all available.

In administrator exec mode, this command is used to manually switch back to fabric modules A, B, and C, when these modules are available. It is used as a manual override when the system is configured with the **no fabric revert** command in global configuration mode. The **no** form of this command is not supported in administrator exec mode.

Examples

The following example configures the system so that it does not automatically switch back to fabric A, B, and C:

```
[local]RedBack#config
[local]RedBack(config)#no fabric revert
[local]RedBack(config)#exit
```

With this configuration, if there is a problem with fabric module B that causes the system to switch to fabric modules A, C, and D, the system does not automatically switch back to fabric modules A, B, and C when fabric module B is replaced. The following example manually switches the system back to the default fabric modules:

```
[local]RedBack#fabric revert
```

Related Commands

show fabric counters

format

format [/*sm*]*device* [**dhcp-secured-arp**]

Purpose

Reformats a device and completely deletes its contents.

Command Mode

administrator exec

Syntax Description

[/*sm*]*device*	Name of the device to be formatted.
dhcp-secured-arp	Optional. Specifies that the device is to be formatted for use as Dynamic Host Configuration Protocol (DHCP) nonvolatile storage. Valid only for PCMCIA synchronous RAM (SRAM) cards.

Default

None

Usage Guidelines

Use the **format** command to reformat a device and completely delete its contents.

The */sm* argument is used only for systems that are configured with redundant System Manager (SM) modules. You can specify files on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the */sm* argument to specify a device on both the active and backup SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform). Only the PCMCIA SRAM devices can be used with the **dhcp-secured-arp** keyword.

Caution This command completely erases all contents of the specified device. Think carefully before reformatting the device that contains the system image and configuration files.

This command is also described in Chapter 29, “DHCP Commands.”

Examples

The following example erases the `/flash` device and reformats it for future use:

```
[local]RedBack#format /flash
```

The following example shows the messages you see when you use the **format** command on a device that already contains a format:

```
[local]RedBack#format /pcmcia0 dhcp-secured-arp

Device /pcmcia0 contains a file system.
Proceed with format of /pcmcia0? [confirm]
```

Press **Enter** (**Return**) to confirm; the system reformats the device as you have specified.

If the device already contains DHCP secured Address Resolution Protocol (ARP) formatting, the messages look like the following example:

```
[local]RedBack#format /pcmcia0

Device /pcmcia0 is formatted for dhcp-secured-arp.
Proceed with format of /pcmcia0? [confirm]
```

Related Commands

directory
mkdir
rmdir

mkdir

mkdir *directory*

Purpose

Creates a new directory on a local file system.

Command Mode

administrator exec

Syntax Description

directory	Name of the directory that is to be created.

Default

None

Usage Guidelines

Use the **mkdir** command to create a new directory on the local file system. You must specify the new directory in the following form:

[*/sm*]*/device*[*/parent*]*/directory*

The */sm* argument is used only on systems that are configured with redundant System Manager (SM) modules. You can create a directory on a device on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the /*sm* specification to specify a device on both the active and backup SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Note When you use the **mkdir** command on a synchronous RAM (SRAM) card that is formatted for Dynamic Host Configuration Protocol (DHCP) secured Address Resolution Protocol (ARP), an error message is displayed and the command is not carried out. The message says that the device is `formatted for dhcp-secured-arp`.

Examples

The following example creates a new top-level directory called `backups` on the flash file system:

```
[local]RedBack#mkdir /flash/backups
```

Related Commands

directory
rename
rmdir

module extract

module extract *slot*

no module extract *slot*

Purpose

Prepares a module for hot-swap extraction.

Command Mode

administrator exec

Syntax Description

slot	Backplane slot number of the module to be replaced.

Default

None

Usage Guidelines

Use the **module extract** command to prepare a module for hot-swap extraction. This command shuts down the ports on the module, removes all circuits and bindings on the module from the running configuration, and places the ports on the module into the EXTRACT_READY state.

When you are prompted, press **y** to confirm this operation.

Note Use the **save configuration** command in administrator exec mode to save the running configuration prior to entering the **module extract** command. For complete instructions on how to hot-swap a module, see the "Loading System Images and Configuration Files" chapter in the *Access Operating System (AOS) Configuration Guide*.

Use the **no** form of this command to cancel a previously entered **module extract** command. The AOS reloads the configuration for the specified slot from memory.

Examples

The following example prepares the module in slot 3 for hot-swap extraction:

```
[local]RedBack#module extract 3
About to prepare module in slot 3 for extraction. Are you sure?[confirm]y
Shutting down ports for slot 3...
```

```
Deleting circuits on port 3/0...
Deleting circuits on port 3/1...
Deleting port 3/0...
Deleting port 3/1...
21:44:41 19Apr2001: %PORTMGR-6-STATECHG: port ds3 3/0 state changed to EXTRACT_READY
21:44:41 19Apr2001: %PORTMGR-6-STATECHG: port ds3 3/1 state changed to EXTRACT_READY
[local]RedBack#
```

Related Commands

configure
save configuration
show hardware
show port table

reload

reload

Purpose

Restarts or reboots the system.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **reload** command to reboot the system. This command causes the system to perform minimal housekeeping, then reload as if powered off and then powered on again.

You can halt the boot process by typing any character within approximately three seconds of entering the **reload** command to access the boot menu. See the “Reload the System” section in the “Loading System Images and Configuration Files” chapter in the *Access Operating System (AOS) Configuration Guide* for additional information.

Examples

The following example reloads the system:

```
[local]RedBack#reload

Proceed with reload? [confirm]

                          ****************************
                          RedBack Networks System Boot
                          ****************************

Version 1.0
Copyright 1998  RedBack Networks, Inc.
Copyright 1984-1996  Wind River Systems, Inc.
```

```
Attaching flash disk device... Message: Verifying Flash Drive
done.
Boot line = dc(0,0):wash/dewy e=192.168.145.35 h=192.168.145.99 f=0x80
Press any key to stop auto-boot...
3
```

Related Commands

boot configuration
boot system
show version

rename

rename *source target* [**-noconfirm**]

Purpose

Renames the file or directory specified as the source to the file or directory name specified as the target.

Command Mode

administrator exec

Syntax Description

source	Name of the source file or directory that is to be renamed.
target	Name of the file or directory after renaming.
-noconfirm	Optional. Replaces an existing file or directory without asking for confirmation.

Default

None

Usage Guidelines

Use the **rename** command to rename a file or directory on the local file system. This command only works for renaming files and directories on a single local file system device. The *source* and *target* arguments use the following form:

[/*sm*]*/device*[/*directory*]/*filename.ext*

The */sm* argument is used only on systems configured with redundant System Manager (SM) modules. You can specify whether to rename a directory or file on a device on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the /*sm* specification to specify a device on both the active and backup SM modules.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Note The *sm* and *device* arguments specified must be identical for the *source* and *target* arguments.

The rename process fails if the source and target have the same name. A file with the new name must not already exist; that is, the AOS does not overwrite an existing file on the flash file system without first seeking confirmation. Use the **-noconfirm** keyword to avoid the confirmation prompt.

Note When you use the **rename** command on a synchronous RAM (SRAM) card that is formatted for Dynamic Host Configuration Protocol (DHCP) secured Address Resolution Protocol (ARP), an error message is displayed and the command is not carried out. The message says that the device is `formatted for dhcp-secured-arp`.

Examples

The following example renames the file named `redback.bin` to `old.bin`. Both files exist on the flash file system.

```
[local]RedBack#rename /flash/redback.bin /flash/old.bin
```

Related Commands

copy
delete
directory

rmdir

rmdir *directory*

Purpose

Removes a directory from the local file system.

Command Mode

administrator exec

Syntax Description

directory	Name of the directory that is to be removed.

Default

None

Usage Guidelines

Use the **rmdir** command to remove a directory on the local file system. When removing a directory, the following form is required:

[/*sm*]/*device*[/*parent*]/*directory*

The */sm* argument is used only on systems configured with redundant System Manager (SM) modules. You can specify whether to remove a directory from a device on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the /*sm* specification to specify a device on both the active and backup SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Before you remove a directory, you must remove all files from the directory using the **delete** command.

Note When you use the **rmdir** command on a synchronous RAM (SRAM) card that is formatted for Dynamic Host Configuration Protocol (DHCP) secured Address Resolution Protocol (ARP), an error message is displayed and the command is not carried out. The message says that the device is `formatted for dhcp-secured-arp`.

Examples

The following example removes the top-level directory called `backups` from the flash file system:

```
[local]RedBack#rmdir /flash/backups
```

Related Commands

delete
directory
mkdir

save configuration

save configuration *url* [**verbose**] [**-noconfirm**]

Purpose

Saves the current configuration of the device to the specified file.

Command Mode

administrator exec

Syntax Description

url	Name of the file to which the configuration is saved.
verbose	Optional. Generates configuration commands for default values.
-noconfirm	Optional. Replaces an existing file without asking for confirmation.

Default

Only those commands that modify the default configuration of the device are saved.

Usage Guidelines

Use the **save configuration** command to save the current configuration of the system to the specified file.

When referring to a file on a File Transfer Protocol (FTP) server, the URL takes the following form, where the *username:passwd* argument specifies the user and an optional password, the *ip-address* argument is the IP address of the FTP server, and the *hostname* argument is the hostname of the FTP server. The **passive** keyword specifies a passive FTP transaction.

ftp://*username*:*passwd*@{*ip-address* | *hostname*}[/*directory*]/*filename.ext* **passive**

When referring to a file on a Trivial File Transfer Protocol (TFTP) server, the URL takes the following form, where the *ip-address* argument is the IP address, or the *hostname* argument is the hostname of the TFTP server:

tftp://{*ip-address* | *hostname*}[/*directory*]/*filename.ext*

The *hostname* argument for TFTP or FTP can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, “DNS Commands.”

When referring to a file on the local file system, the URL takes the following form:

[**file:**][/*sm*]/*device*[/*directory*]/*filename.ext*

The */sm* argument is used only on systems configured with redundant System Manager (SM) modules. You can specify whether to remove a directory from a device on the active SM module, on a particular SM module, or on both the active and backup SM modules as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the /*sm* specification to specify a device on both the active and backup SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Use the **verbose** keyword to generate configuration commands for all default values. Usually this keyword is not specified because it can lead to a large increase in the size of the generated configuration file.

Use the **-noconfirm** keyword to replace an existing file without providing confirmation to the system.

Examples

The following example saves the current active system configuration to a file named `aos.cfg` on the local file system:

```
[local]RedBack#save configuration /flash/aos.cfg
```

Related Commands

ip domain-lookup
ip domain-name
ip name-servers
show configuration

show configuration

show configuration [*url* | **context** *ctx-name* | **port** *slot/port* | **tunnel** *tun-name*] [**verbose**]

Purpose

Displays either the current configuration of the device or a previously saved configuration.

Command Mode

administrator exec

Syntax Description

url	Optional. Name of a configuration file to be displayed.
context *ctx-name*	Optional. Name of the context whose configuration is to be displayed.
port *slot/port*	Optional. Backplane slot number and port number of the port to be displayed.
tunnel *tun-name*	Optional. Name of the tunnel to be displayed.
verbose	Optional. Includes configuration commands for default values in the display.

Default

The running configuration is displayed, and includes only those commands that are required to modify the default configuration of the device.

Usage Guidelines

Use the **show configuration** command to display the current system configuration or a previously saved configuration. When referring to a file on a Trivial File Transfer (TFTP) server, the URL takes the following form, where the *ip-address* argument is the IP address, or the *hostname* argument is the hostname of the TFTP server:

tftp://{*ip-address* | *hostname*}[/*directory*]/*filename.ext*

When referring to a file on a File Transfer Protocol (FTP) server, the URL takes the following form, where the *username:passwd* argument specifies the user and an optional password, the *ip-address* argument is the IP address of the FTP server, and the *hostname* argument is the hostname of the FTP server. The **passive** keyword specifies a passive FTP transaction.

ftp://*username*:*passwd*@{*ip-address* | *hostname*}[/*directory*]/*filename.ext* **passive**

The *hostname* argument for TFTP or FTP can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, “DNS Commands.”

When referring to a file on the local file system, the URL takes the following form:

[**file:**][*/sm*]*/device*[*/directory*]*/filename.ext*

The */sm* argument is used only on systems configured with redundant System Manager (SM) modules. You can specify whether to display a configuration file on the active SM module, or on a particular SM module as follows:

- Specify /**sm** to specify a device on the active SM module.
- Specify /**sm2** or /**sm3** to specify a device on a particular SM module.
- Omit the /*sm* specification to specify a device on the active SM module.

The *device* argument can be /flash, /pcmcia0, or /pcmcia1 (depending on your hardware platform).

Usually the **verbose** keyword is not specified because it can lead to a large increase in the amount of output.

Examples

The following example displays the entire active configuration of the system, including default values:

```
[local]RedBack#show configuration verbose
```

The following example displays the active configuration of the system:

```
[local]RedBack#show configuration
```

The following example displays a previously saved configuration file named `full.cfg`:

```
[local]RedBack#show configuration /flash/full.cfg
```

Related Commands

boot configuration
ip domain-lookup
ip domain-name
ip name-servers
save configuration

show version

show version

Purpose

Displays information about the system software and uptime.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show version** command to display the current software version, the system uptime, and the reason for the last system reload.

Examples

The following example shows sample output from the **show version** command:

```
[local]RedBack>show version
RedBack Networks AOS Release 3.0.3.0 PRODUCTION RELEASE
Copyright (c) 1997-1999 by RedBack Networks, Inc.
Compiled 1999-Jul-26 15:14:19 GMT by rick
Image text-base: 0x00108000, data-base: 0x00460388

System Bootstrap Version unknown (pre-1.6)

RedBack uptime is 1 week, 1 day, 3 hours, 45 minutes
System restarted by reload at 18:45:34 Mon Aug 2 1999
System image file is "redback.bin", booted via tftp from 10.1.1.1
```

Related Commands

show configuration

Basic System Commands

This chapter describes, in detail, the configuration commands that provide you with basic system information concerning the Subscriber Management System (SMS) device. The commands provided in this section identify and locate the system being used, set the time and date, and relay any relevant system messages to the operator or administrator.

For overview information, a description of the tasks used to configure, and configuration examples, see the "Configuring Basic System Parameters" chapter in the *Access Operating System (AOS) Configuration Guide*.

banner motd

banner motd *delimited-text*

no banner motd

Purpose

Specifies a message of the day (MOTD) to be displayed when an administrator or operator connects to the system.

Command Mode

global configuration

Syntax Description

delimited-text	The text to be displayed. You can use any character to delimit the text.

Default

No banner MOTD is defined.

Usage Guidelines

Use the **banner motd** command to display a message to administrators or operators.

Use the **no** form of this command to delete the message.

Examples

The following example configures a message to be displayed when an administrator or operator connects to the system:

```
[local]RedBack(config)#banner motd /Welcome to Redback SMS/
```

Related Commands

show administrators

clock set

clock set *yyyy:mm:dd:hh:mm*[*:ss*]

Purpose

Sets the system clock.

Command Mode

administrator exec

Syntax Description

yyyy:mm:dd:hh:mm[*:ss*]	Year, month, day, hour, minutes, and, optionally, seconds. The hour is in a 24-hour format; for example, 6:00 p.m. is 18:00.

Default

None

Usage Guidelines

Use the **clock set** command to set the system clock. The time is saved in a hardware real-time clock and is preserved across system reloads. This clock is used for all system timestamps, such as in log messages.

Examples

The following example sets the clock to 12:01 p.m. on `7/04/98`:

```
[local]RedBack#clock set 1998:07:04:12:01
```

Related Commands

show clock

clock summer-time

clock summer-time *zone1 zone2* {**recurring** *week day month hh week day month hh* | **date** *yyyy:mm:dd:hh:mm yyyy:mm:dd:hh:mm*}

no clock summer-time *zone1 zone2* {**recurring** *week day month hh week day month hh* | **date** *yyyy:mm:dd:hh:mm yyyy:mm:dd:hh:mm*}

Purpose

Configures the system to automatically switch to daylight savings time or summer time.

Command Mode

global configuration

Syntax Description

zone1	Name of the time zone to which this adjustment applies; for example, Pacific Standard Time (PST).
zone2	Name of the time zone to be displayed when summer time is in effect; for example, Pacific Daylight Time (PDT).
week	Week of the month (**first**, 1 to 4, or **last**).
day	Day of the week; for example, Sunday, Monday, and so on.
month	Month of the year; for example, January, February, and so on.
hh	Hour of the day, expressed in a 24-hour format; for example, 6:30 p.m. is expressed as 18:30.
yyyy:dd:hh:mm	Year, the date, and the time for hours and minutes expressed in a 24-hour format; for example, 6:30 p.m. is expressed as 18:30.

Default

Daylight Savings Time is disabled by default. If the **recurring** keyword is not followed by date information, the rules for the United States are applied. The offset applied is 60 minutes.

Usage Guidelines

Use the **clock summer-time** command to set the system to automatically switch to Daylight Savings Time when displaying time.

Use the **recurring** keyword if the rules for switching to summer time are applied in precisely the same way each year. The first set of variables (*week, day, month, hh*) refers to the start day; the second set (*yyyy:mm:dd:hh:mm yyyy:mm:dd:hh:mm*) refers to the end day.

Note You must use the **recurring** keyword with a specified date, because the system default (U.S. summer time) cannot be deleted. If you delete the timezone for which the summer time information is specified (using the **no clock timezone** command), the summer time information is deleted. In addition, the relevant **clock summer-time** command is removed from the configuration file.

Alternatively, you can use the **date** keyword to specify a start and end date for summer time. In the **date** format, you can specify start and end dates for multiple years at the same time, as long as the timezones to which the dates apply are unique and there is no overlap of dates. The start time is relative to standard time and the end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere. The entry for the *zone1* argument must be a previously configured timezone (using the **clock timezone** command). Use the string for the *zone2* argument when summer time is in effect.

Use the **no** form of this command to delete information provided for the named zone and for the named year.

Examples

The following example configures summer time is to start on the first `Sunday` in `April` at 7 a.m. and end on the last `Sunday` in `October` at 3 a.m. for the `PST` and `MST` timezones (previously defined using the **clock timezone** command):

```
[local]RedBack#config
[local]RedBack(config)#clock summer-time PST PDT recurring 1 Sunday April 7 last Sunday
October 3
[local]RedBack(config)#clock summer-time MST MDT recurring 1 Sunday April 3 last Sunday
October 3
```

Another example for a southern hemisphere location is:

```
[local]RedBack#config
[local]RedBack(config)#clock summer-time AST ADT date 1999:10:12:02:00 2000:04:28:02:00
```

The following example deletes the summer time information for the `AST` timezone:

```
[local]RedBack#config
[local]RedBack(config)#no clock summer-time AST ADT date 1999:10:12:02:00
2000:04:28:02:00
```

Related Commands

clock set
clock timezone
show clock

clock timezone

clock timezone *zone hours* [*minutes*] [**local**]

no clock timezone *zone hours* [*minutes*] [**local**]

Purpose

Defines one or more timezones and their distances from Coordinated Universal Time (UTC) for display purposes.

Command Mode

global configuration

Syntax Description

zone	Name of the time zone to be displayed when standard time is in effect; for example, Pacific Standard Time (PST).
hours	Number of hours offset from UTC. The range of values is -23 to 23.
minutes	Optional. Number of minutes offset from UTC. The range of values is 0 to 59; the default is 0.
local	Optional. Specifies that the timezone being specified is the local timezone.

Default

The default timezone is UTC. If no timezone is configured with the **local** keyword, the system uses UTC when displaying time.

Usage Guidelines

Use the **clock timezone** command to define one or more timezones and their distances from UTC. The system keeps time in UTC and the local timezone specified is displayed. The local timezone specified is also used when you execute the **clock set** command. You can specify multiple timezones; the only timezone assumed to be local is the one with the **local** keyword.

Use the **no clock timezone** *zone* command to delete previously configured timezone information. If the named timezone is the one specified as the local timezone, the system reverts to displaying UTC time.

Use the **no clock timezone** command with no parameters specified to remove all previously configured timezone and corresponding daylight savings information.

Examples

The following example defines Atlantic Standard Time (AST), Eastern Standard Time (EST), Central Standard Time (CST), Mountain Standard Time (MST), Pacific Standard Time (PST), and Hawaii Standard Time (HST) timezones. PST is also specified as the local timezone.

```
[local]RedBack(config)#clock timezone AST –4
[local]RedBack(config)#clock timezone EST –5
[local]RedBack(config)#clock timezone CST –6
[local]RedBack(config)#clock timezone MST –7
[local]RedBack(config)#clock timezone PST –8 local
[local]RedBack(config)#clock timezone HST –10
```

The following example deletes the EST timezone information:

```
[local]RedBack(config)#no clock timezone EST
```

Related Commands

clock set
clock summer-time
show clock

configure

configure [*url* [**verbose**]]

Purpose

Enters global configuration mode or configures the system from a pre-existing configuration file.

Command Mode

administrator exec

Syntax Description

url	Optional. URL of a pre-existing configuration file.
verbose	Optional. Displays each line and its line number when configuring from a pre-existing configuration file.

Default

Enters global configuration mode.

Usage Guidelines

Use the **configure** command to enter global configuration mode or to configure the system from a configuration file. If the *url* argument is not specified, the system enters global configuration mode. If the *url* argument is specified, configuration commands are read from the associated file.

When referring to a file on the local file system, the URL takes the following form:

[**file:**][**/sm**]*/device*[*/directory*]*/filename.ext*

The **/sm** specification applies only to systems that are configured with redundant System Manager (SM) modules. You can only specify an image file on the active SM module.

The *device* argument can be **/flash**, **/pcmcia0**, or **/pcmcia1** (depending on your hardware platform).

When referring to a file on a Trivial File Transfer Protocol (TFTP) server, the URL takes the following form, where the *ip-address* argument is the IP address, or the *hostname* argument is the hostname of the TFTP server:

tftp://{*ip-address* | *hostname*}[*/directory*]*/filename.ext*

The *hostname* argument can only be used if the Domain Name System (DNS) is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode; see Chapter 28, “DNS Commands.”

After you enter the **configure** command, the system prompt changes from [*context*]*hostname*# to [*context*]*hostname* (config)#, where the *hostname* argument is the local hostname, indicating that you are in global configuration mode. To leave global configuration mode and return to the administrator exec prompt, use the **end** command.

Examples

The following example enters global configuration mode:

```
[local]RedBack#configure

Enter configuration commands, one per line, 'end' to exit
[local]RedBack(config)#
```

The following example configures the system from a configuration file on the local file system:

```
[local]RedBack#configure /flash/old_config.cfg
```

Related Commands

exit
ip domain-lookup
ip domain-name
ip name-servers
save configuration

privilege

privilege *mode* [**inherit**] **level** *level command*

{**no** | **default**} **privilege** *mode command*

Purpose

Configures the privilege level for the specified command.

Command Mode

global configuration

Syntax Description

mode	Mode of the command to be configured.
inherit	Optional. Assigns the specified privilege level to all keywords that follow the last keyword specified in the *command* argument.
level *level*	Minimum privilege level required to execute the specified command. The range of values is 0 to 15.
command	Command keyword (or keywords).

Default

Operator exec commands are set to privilege level 3. Administrator exec and configuration commands are set to privilege level 10.

Usage Guidelines

Use the **privilege** command to modify the privilege level for a specific command or set of commands.

Use the **inherit** keyword as a shortcut to modify all commands beginning with one or more keywords. For example, to modify all commands beginning with the **aaa** keyword (**aaa accounting**, **aaa authentication**, and so on), specify the **inherit** keyword, and specify **aaa** for the command argument.

Use the **no** or **default** form of this command to return a command to the default privilege level.

Examples

The following command sets the `privilege level` for the **reload** command to the highest privilege level:

```
[local]RedBack(config)#privilege exec level 15 reload
```

The following command sets the `privilege level` for all **aaa** commands to `12`:

```
[local]RedBack(config)#privilege global inherit level 12 aaa
```

Related Commands

privilege max
privilege start
show privilege

show clock

show clock [**universal**]

Purpose

Displays the current system time of day clock.

Command Mode

operator exec

Syntax Description

universal	Optional. Displays the time in Coordinated Universal Time (UTC).

Default

Displays time in local time.

Usage Guidelines

Use the **show clock** command to display the current system time of day clock. The time displayed is based on configuration information provided using the **clock set** and the **clock timezone** commands. If no timezone is configured as the local timezone, the system uses UTC as the default timezone. If a local timezone is configured, you can also display UTC using the **universal** keyword.

Examples

The following is sample output from the **show clock** command:

```
[local]RedBack>show clock

TUE JUN 29 10:01:06 PST 1999
[local]RedBack>show clock universal

TUE JUN 29 18:01:06 UTC 1999
```

Related Commands

clock set
clock summer-time
clock timezone

system contact

system contact *text*

{**no** | **default**} **system contact**

Purpose

Sets the system contact string.

Command Mode

global configuration

Syntax Description

text	Text that explains whom to contact, and how, for information regarding the system.

Default

No system contact information is specified by default.

Usage Guidelines

Use the **system contact** command to configure the information available via the sysContact Management Information Base (MIB)-II object. The *text* argument can be any alphanumeric string, including spaces. The *text* can not be longer than one line.

Use the **no** or **default** form of this command to remove system contact information.

Examples

The following example sets a contact string:

```
[local]RedBack(config)#system contact IS Hotline 1-800-555-1567
```

Related Commands

system hostname
system location

system hostname

system hostname *name*

default system hostname

Purpose

Modifies the system hostname.

Command Mode

global configuration

Syntax Description

name	Alphanumeric string to be used as the hostname for the system.

Default

The factory-assigned default hostname is RedBack.

Usage Guidelines

Use the **system hostname** command to modify the system hostname. Do not expect case to be preserved. Uppercase and lowercase characters look the same to many Internet software applications. It might seem appropriate to capitalize a name, the same way you do in English, but conventions dictate that computer names appear as all lowercase. For more information, see RFC 1178, *Choosing a Name for Your Computer*.

The name must also follow the rules for Advanced Research Projects Agency Network (ARPANET) hostnames. Names must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. For more information, see RFC 1035, *Domain Names—Implementation and Specification*.

Use the **default** form of this command to set the hostname to the default name.

Examples

The following example changes the hostname to `freebird`:

```
[local]RedBack(config)#system hostname freebird
[local]freebird(config)#
```

Related Commands

show version

system location

system location *text*

{**no** | **default**} **system location**

Purpose

Sets the system location string.

Command Mode

global configuration

Syntax Description

text	Text that explains the physical location of the system.

Default

No system location is specified by default.

Usage Guidelines

Use the **system location** command to configure the information available via the sysLocation MIB-II object. The *text* argument can be any alphanumeric string, including spaces. The *text* can not be longer than one line.

Use the **no** or **default** form of this command remote system location information.

Examples

The following example sets a location string:

```
[local]RedBack(config)#system location Building 3, 2nd Floor, Lab 3
```

Related Commands

system contact
system hostname

Part 2

Setting Up Contexts with Interfaces and Subscribers

Context Commands

This chapter describes the basic commands used to configure and maintain contexts supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure contexts, and configuration examples, see the "Configuring Contexts" chapter in the *Access Operating System (AOS) Configuration Guide*.

administrator

administrator *name* [**password** *password*]

no administrator *name*

Purpose

Configures an administrator logon account, secures the console port, enables Telnet and Secure Shell (SSH), and enters administrator configuration mode.

Command Mode

context configuration

Syntax Description

administrator *name*	Alphanumeric string indicating administrator username.
password *password*	Optional. Alphanumeric string indicating the administrator password. This password is used both for initial logon and **enable** verification.

Default

No administrator accounts are defined.

Usage Guidelines

Use the **administrator** command to configure an administrator account. You must specify the *password* argument when creating a new administrator account.

Administrators can log on directly to the console and through Telnet and can use the **enable** command to modify the exec privilege level.

You can enter a password with embedded spaces by enclosing the entire password in double quotation marks; for example, `"This is a Password With Spaces"`.

Note When the system generates the configuration, this command appears with an encrypted password in the file. Passwords are never displayed in readable text.

Use the **no** form of this command to remove the named administrator account.

Examples

The following example configures an administrator with a username of `admin` and a password of `supersecret`:

```
[local]RedBack(config-ctx)#administrator admin password supersecret
[local]RedBack(config-admin)#
```

Related Commands

aaa authentication administrator
enable

clear ip counter

clear ip counter

Purpose

Clears all IP traffic statistics associated with the **show ip traffic** command in the current context.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **clear ip counter** command to clear all IP traffic statistics in the current context. This command only affects the traffic statistics in the current context available to the command line. Corresponding Simple Network Management Protocol (SNMP) counters are not cleared.

Examples

The following command clears the IP traffic counters:

```
[local]RedBack#clear ip counter
```

Related Commands

show ip traffic

context

context *name*

no context *name*

Purpose

Creates a context with the specified name (if the context does not already exist) and enters context configuration mode.

Command Mode

global configuration

Syntax Description

name	Alphanumeric string to be used as the name for the new context or the name of an existing context.

Default

The local context is defined.

Usage Guidelines

Use the **context** command to create or modify a context.

The context named `local` has special meaning and is always present. Only an administrator authenticated in the local context can configure the system. Operators and administrators authenticated in the local context can observe any portion of the system, regardless of context. Operators and administrators authenticated in other contexts are restricted to that portion of the system that is relevant to the particular context.

Contexts are completely independent name spaces and data spaces. For example, the same subscriber name may appear in two different contexts; a routing process in one context will not share routing information with a routing process in another context, and vice versa.

When you enter this command to create a new context, the Access Operating System (AOS) checks the amount of memory available on the Forwarding Engine (FE) module (on systems that are configured with an FE module). If the context to be configured will consume most of the available memory, the AOS displays a warning message and then creates the context. If there is not enough memory to create the context, the AOS displays an error message and does not allow you to create the new context.

Use the **no** form of the command to delete the named context and all configuration information associated with it.

Examples

The following example shows how to enter context configuration mode to configure the local context:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#
```

The following example creates a new context called `corp.com` is created, and enters context configuration mode to configure the `corp.com` context:

```
[local]RedBack(config)#context corp.com
[local]RedBack(config-ctx)#
```

Related Commands

domain

domain

domain *alias* [**advertise**]

no domain *alias*

Purpose

Configures a domain-name alias for a context.

Command Mode

context configuration

Syntax Description

alias	Unique ASCII-string alias for the context.
advertise	Specifies that this domain is advertised as a service in Point-to-Point Protocol over Ethernet (PPPoE) Active Discovery Offer (PADO) packets sent by AOS if the **pppoe services** command is enabled with the **marked-domains** keyword.

Default

No aliases are defined.

Usage Guidelines

Use the **domain** command to add an alias for the context that can referenced by usernames during authentication. When one or more domain values are configured, a subscriber can authenticate as *username@context_name* or *username@domain_name* and, in both cases, will be associated with the same context.

If the **pppoe services** command is not set to **marked-domains**, the **advertise** keyword has no effect. When the **pppoe services** command is set to **all-domains**, all tunnel alias names are advertised in PADO packets.

Use the **no** form of this command to remove the domain-name alias from the context.

Examples

The following example sets an authentication domain alias of `retail.com`. Subscribers can log on as *`username`*`@retail` or *`username`*`@retail.com`.

```
[local]RedBack(config)#context retail
[local]RedBack(config-ctx)#domain retail.com
```

The following example shows how to advertise only the domains corp3 and corp4:

```
[local]RedBack(config)#context corp3.com
[local]RedBack(config-ctx)#domain corp3 advertise
[local]RedBack(config-ctx)#exit
[local]RedBack(config)#context corp4.com
[local]RedBack(config-ctx)#domain corp4 advertise
[local]RedBack(config-ctx)#exit
[local]RedBack(config)#pppoe services marked-domains
```

Related Commands

context
pppoe services

ip access-group

ip access-group *name* {**in** | **out**}

no ip access-group *name*

Purpose

Applies an access control list to a context, restricting administrative access to the system.

Command Mode

context configuration
interface configuration
subscriber configuration

Syntax Description

name	Name of the access list to be applied.
in	Applies the access group to packets received by the context.
out	Applies the access group to packets sent by the context.

Default

All packets to and from a context are permitted.

Usage Guidelines

Use the **ip access-group** context configuration command to apply an IP access control list to a context. This type of access control list is called an *administrative access control list*. With this command, unauthorized access *to* the administration (for example, Telnet, Simple Management Network Protocol (SNMP), Internet Control Message Protocol (ICMP), and HTTP access) of the system can be prevented. Use the **ip access-list** command to create the access control list and enter access control list configuration mode where you can define conditions using the **permit** and **deny** commands.

Use the **ip access-group** interface configuration command to apply an access list to an interface, restricting the flow of traffic *through* the system. Likewise, the **ip access-group** subscriber configuration command applies an access list to a subscriber, restricting the flow of traffic *through* the system.

This command is repeated in Chapter 37, “IP Access Control List Commands.”

Use the **no** form of this command to remove an applied access control list from a context.

Examples

The following example disables Telnet (TCP port 23) access to the SMS context `corp3.com`:

```
[local]RedBack(config)#context corp3.com
[local]RedBack(config-ctx)#ip access-list Corp3AdminACL
[local]RedBack(config-acl)#deny tcp any any eq 23
[local]RedBack(config-acl)#permit any
[local]RedBack(config-acl)#exit
[local]RedBack(config-ctx)#ip access-group Corp3AdminACL in
```

Related Commands

ip access-group
ip access-list

operator

operator *name* **password** *password*

no operator *name*

Purpose

Configures an operator system logon account.

Command Mode

context configuration

Syntax Description

name	Alphanumeric string indicating the operator username.
password	Alphanumeric string defining the operator password.

Default

No operator accounts are defined.

Usage Guidelines

Use the **operator** command to create an operator account. Operators are allowed to log on directly to the console and through Telnet or Secure Shell (SSH). By default, operators have lower privilege levels than administrators.

When the system generates the configuration, the **operator** command appears in a different form with an encrypted password. Passwords are never displayed in readable text.

You can enter a password with embedded spaces by enclosing the entire password in double quotes; for example, `"This is a Password With Spaces"`.

Use the **no** form of this command to delete an existing operator account.

Examples

The following example configures an operator logon with the name `operat` and password `supersecret`:

```
[local]RedBack(config-ctx)#operator operat password supersecret
```

Related Commands

aaa authentication administrator
administrator
enable

privilege max

privilege max *level*

default privilege max

Purpose

Configures the maximum privilege level for the operator or administrator.

Command Mode

administrator configuration

Syntax Description

level	Maximum privilege level for an administrator or operator. The range of values is 0 to 15.

Default

The maximum privilege level is set to 6 for operators and 15 for administrators.

Usage Guidelines

Use the **privilege max** command to configure the maximum privilege level for the operator or administrator.

Use the **default** form of this command to return the maximum privilege level for an operator or administrator back to the default value.

Examples

The following command configures administrator `fred` to a maximum privilege level of `13`:

```
[local]RedBack(config)# administrator fred
[local]RedBack(config-admin)# privilege max 13
```

Related Commands

enable
privilege
privilege start
show privilege

privilege start

privilege start *level*

Purpose

Configures the initial privilege level for exec sessions initiated by an operator or administrator.

Command Mode

administrator configuration

Syntax Description

level	Initial privilege level for exec sessions initiated by an operator or administrator. The range of values is 0 to 15.

Default

The initial privilege level is set to 6 for operators and 15 for administrators.

Usage Guidelines

Use the **privilege start** command to configure the initial privilege level for exec sessions initiated by the operator or administrator.

Use the **default** form of this command to return the initial privilege level for an operator or administrator back to the default value.

Examples

The following command configures administrator `fred` with an initial privilege level of `11`:

```
[local]RedBack(config)#administrator fred
[local]RedBack(config-admin)#privilege start 11
```

Related Commands

enable
privilege
privilege max
show privilege

show context

show context [*context-name* | **all**]

Purpose

Displays configured context names.

Command Mode

operator exec

Syntax Description

context-name	Optional. Name of a context to be displayed.
all	Optional. Displays all context names.

Default

Displays the current context name.

Usage Guidelines

Use the **show context** command to see if a particular context has been configured or to get a listing of all the configured contexts. When used without any optional argument, it shows the name of the current context.

Examples

The following commands show sample output for the **show context** command:

```
[isp-a]RedBack>show context

isp-a(1)
[isp-a]RedBack>show context isp-a

isp-a(1)
[isp-a]RedBack>show context all

local(0)
isp-a(1)
```

Related Commands

context

show ip host

show ip host [*ip-address*]

Purpose

Displays information about statically configured IP hosts in the current context.

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address of the Host table entry to display, in the form A.B.C.D.

Default

Displays all IP host table entries.

Usage Guidelines

Use the **show ip host** command to display information about statically configured IP hosts in the current context. If the optional *ip-address* argument is not specified, the entire IP host table is displayed. Otherwise, only the host entry matching the *ip-address* argument is displayed.

IP host entries or subscriber records must be configured in order to take advantage of the secured-Address Resolution Protocol (ARP) feature of the Access Operating System (AOS).

Examples

The following shows sample output from the **show ip host** command:

```
[local]RedBack>show ip host

Host        Nexthop      Nhop cct  Source  Mac address        State
10.3.7.10   10.3.7.54    30000001  Arp     00:60:97:a1:5a:a3  up
10.3.7.11   10.3.7.54    30000001  Arp     00:a0:24:dd:a4:46  up
10.3.7.14   10.3.7.54    30000001  Arp     00:a0:24:c8:92:9f  up
10.3.7.17   10.3.7.54    30000001  Arp     00:a0:24:bf:8c:5c  up
10.3.7.18   10.3.7.54    30000001  Arp     00:00:a0:0b:04:07  up
10.3.7.54   local        local     System  00:10:67:00:04:07  up
10.3.254.53 local        local     System  00:10:67:00:00:04  up
10.3.254.54 10.3.254.53  31000001  Arp     00:e0:1e:8d:1e:d8  up
```

Related Commands

show ip arp
show ip secured-arp
ip host

show ip traffic

show ip traffic [**arp** | **general** | **icmp** | **igmp** | **tcp** | **udp**]

Purpose

Displays IP packet statistics for the current context.

Command Mode

operator exec

Syntax Description

arp	Optional. Displays only a summary of Address Resolution Protocol (ARP) statistics.
general	Optional. Displays only a summary of general IP statistics.
icmp	Optional. Displays only a summary of Internet Control Message Protocol (ICMP) statistics.
igmp	Optional. Displays only a summary of Internet Group Management Protocol (IGMP) statistics.
tcp	Optional. Displays only a summary of Transmission Control Protocol (TCP) statistics.
udp	Optional. Displays only a summary of User Datagram Protocol (UDP) statistics.

Default

Displays a summary of traffic statistics for all IP protocols.

Usage Guidelines

Use the **show ip traffic** command to display IP traffic statistics. The IP traffic statistics are gathered for traffic destined to the system itself and do not include forwarded traffic.

Examples

The following example displays all UDP traffic destined to, or sourced by the system:

```
[local]RedBack>show ip traffic udp

UDP statistics:
     Rcvd:  534 total, 0 bad format
            0 checksum errors, 521 no port
            0 full socket 1 pcb lookup failure
     Sent: 12 total
```

Related Commands

clear ip counter
show port counters

show privilege

show privilege

Purpose

Displays the privilege level for the current exec session.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show privilege** command to display the current privilege level for the exec session.

Examples

The following command shows sample output from the **show privilege** command:

```
[local]RedBack>show privilege

The current privilege level is 15
```

Related Commands

enable
privilege max
privilege start

timeout

timeout {**absolute** | **idle**} *minutes*

[**default** | **no**] **timeout**

Purpose

Sets the idle or absolute timeout for the administrator's Telnet or console session.

Command Mode

administrator configuration

Syntax Description

absolute	Specifies an absolute timeout.
idle	Specifies an idle timeout.
minutes	Number of minutes before the session expires. The range is 10 through 596,523.

Default

No timeout is defined.

Usage Guidelines

Use the **timeout** command to configure either an absolute or idle timeout for the administrators' Telnet or console session.

Use the **default** or **no** form of this command to remove the timeout for the administrator.

Examples

The following example configures an administrator named `joe` who can maintain a Telnet or console session for only `15` minutes before he is logged off the system:

```
[local]RedBack(config-ctx)#administrator joe password 5hwpv4l
[local]RedBack(config-admin)#timeout absolute 15
```

Related Commands

administrator
radius timeout

Interface Commands

This chapter describes the commands used to configure, maintain, and troubleshoot interfaces through the Access Operating System (AOS); specifically, commands to configure IP addresses, IP address pools, and parameters for the Address Resolution Protocol (ARP), the Internet Control Message Protocol (ICMP), and maximum transmission unit (MTU) size.

Note For feature-specific interface configuration mode commands, see the appropriate chapter in this guide. For example, to enable interfaces to originate Internet Group Management Protocol (IGMP) queries and use IGMP responses from hosts, see Chapter 36, "IGMP Proxy Commands."

For overview information, a description of the tasks used to configure interfaces, and configuration examples, see the "Configuring Interfaces" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug ip arp

debug ip arp

no debug ip arp

Purpose

Enables the logging of IP Address Resolution Protocol (ARP) debug messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Usage Guidelines

Use the **debug ip arp** command to enable the logging of IP ARP debug messages. You can use the **logging console** and **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables the logging of IP ARP debug messages:

```
[local]RedBack#debug ip arp
```

Related Commands

ip arp arpa
logging console
show ip arp
terminal monitor

debug ip interface

debug ip interface

no debug ip interface

Purpose

Enables the logging of debug messages for IP interfaces.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Usage Guidelines

Use the **debug ip interface** command to enable the logging of debug messages for IP interfaces. Use the **logging console** and **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables the logging of debug messages for IP interfaces:

```
[local]RedBack#debug ip interface
```

Related Commands

interface
ip address—interface configuration mode
logging console
show ip interface
terminal monitor

debug ip secured-arp

debug ip secured-arp

no debug ip secured-arp

Purpose

Enables the logging of IP secured Address Resolution Protocol (ARP) debug messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Usage Guidelines

Use the **debug ip secured-arp** command to enable the logging of IP secured ARP debug messages. Use the **logging console** and **terminal monitor** commands to display the messages in real time

.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables the logging of IP secured ARP debug messages:

```
[local]RedBack#debug ip secured-arp
```

Related Commands

ip secured-arp
logging console
show ip secured-arp
terminal monitor

description

description *text*

no description

Purpose

Assigns a text description to an interface.

Command Mode

interface configuration

Syntax Description

text	Text string that identifies the interface.

Default

None

Usage Guidelines

Use the **description** command to assign a text description to an interface. The description appears in the output of the **show interface** and **show configuration** commands. Text can be any alphanumeric string, including spaces, that is no longer than one line. Text should not wrap to the next line.

Use the **no** form of this command to remove the description from the interface.

Examples

In the following example, the interface named `upstream` is the upstream interface to the `goldisp.net` service provider:

```
[local]RedBack(config)#interface upstream
[local]RedBack(config-if)#description interface to goldisp.net
```

Related Commands

show configuration
show ip interface

interface

interface *if-name* [**loopback**] [**ppp-default**]

no interface *if-name*

Purpose

Configures an interface name and, optionally, to specify the interface as a loopback interface or a default PPP interface. Also enters interface configuration mode.

Command Mode

context configuration

Syntax Description

if-name	Name of the interface. An alphanumeric string.
loopback	Optional. Specifies that the interface is a loopback interface.
ppp-default	Optional. Creates a default Point-to-Point Protocol (PPP) interface that acts as a fall back for incoming PPP connections.

Default

None

Usage Guidelines

Use the **interface** command to configure an interface name and, optionally, to specify the interface as a loopback interface or a default PPP interface. This command also causes the configuration mode to change to interface configuration mode.

Once created, any interface (other than a loopback interface) must be assigned an IP address and bound to a specific circuit. A loopback interface is an interface that has no association with any circuit in the system. This is useful in applications that require an IP address in a particular context, but not necessarily a physical connection. For instance, loopback interfaces can be useful for routing protocols, because the interface is not associated with a physical port that can go down. You can use only the **ip address** and **description** interface configuration commands for a loopback interface. You cannot configure secondary IP addresses for a loopback interface. You can define up to 16 loopback interfaces per context.

Ordinarily, PPP sessions that attempt to come up and cannot bind to a valid interface simply fail. A PPP default interface acts as a fall back for those incoming PPP connections. If a PPP session is established, and there is no valid interface to which it can bind, the session binds to the default interface. The default interface is a virtual interface; there is no actual outgoing circuit. Therefore, a proxy is necessary. One or

more interfaces that are not the default interface are set up as proxies using the **ip ppp-proxy-arp** command. The outgoing circuits from these proxies can then be used to handle the traffic on the virtual default interface.

You must assign an IP address to the PPP default interface, but you cannot enter a subnet mask. The netmask is always assumed to be 255.255.255.255. You cannot configure secondary IP addresses for a PPP default interface. You can only use the following interface configuration commands for a PPP default interface: **description**, **ip address**, **ip access-group**, **ip igmp**, and **ip mtu**.

Use the **no** form of this command to delete the interface.

Caution Deleting an interface removes all bindings to the interface. If more than one circuit is bound to an interface, the Subscriber Management System (SMS) device does not send Routing Information Protocol (RIP) updates on any of those circuits.

Examples

The following example configures an interface with the name `enet1`:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip address 10.1.1.1 255.255.255.0
```

The following example configures a loopback interface for the local context called `local-loopback`:

```
[local]RedBack(config-ctx)#interface local-loopback loopback
[local]RedBack(config-if)#ip address 10.1.1.1 255.255.255.0
```

The following example configures the interface `ppp-connections` as the PPP default interface:

```
[local]RedBack(config-ctx)#interface ppp-connections ppp-default
[local]RedBack(config-if)#ip address 10.1.1.1
```

The following example deletes an interface with the name `atm3`:

```
[local]RedBack(config-ctx)#no interface atm3
[local]RedBack(config-if)#
```

Related Commands

bind interface
debug ip interface
ip address—interface configuration mode
ip ppp-proxy-arp
show ip interface

ip address

ip address *ip-address* [*netmask*] [**secondary**]

no ip address *ip-address*

Purpose

Configures the primary or secondary IP address and netmask for the specified interface.

Command Mode

interface configuration

Syntax Description

ip-address	Primary IP address of the interface.
netmask	Optional. Network mask for the associated IP network. This argument is required, except for loopback interfaces. If a value is not specified for a loopback interface, the default *netmask* argument is 255.255.255.255.
secondary	Optional. Configures the address and network mask as a secondary IP address assigned to the interface.

Default

None

Usage Guidelines

Use the **ip address** command to configure the primary or secondary IP address netmask for the specified interface. Assign the interface a primary IP address and netmask using the *ip-address* and *netmask* arguments. Then bind a circuit to the interface on which IP services are enabled using a **bind** command. You cannot enter a netmask for a Point-to-Point (PPP) default interface. The netmask is always assumed to be 255.255.255.255.

Use the **secondary** keyword to tag the IP address and network mask as a secondary IP address for the interface. You can configure up to 15 secondary addresses per primary interface. Secondary IP addresses allow a subscriber's circuit to bind to two or more noncontiguous Classless InterDomain Routing (CIDR) address blocks. Secondary IP addresses are typically created when there is a scarcity of IP addresses, and new address ranges must be configured to support a growing number of subscribers. You cannot configure secondary addresses for loopback interfaces or for PPP default interfaces. Interface costs configured for routing protocols apply to secondary IP addresses in the same manner that they apply to primary IP addresses. Secondary IP addresses are treated as locally attached networks.

To assign an IP address from a pool of addresses, use the **ip pool** command.

If Routing Information Protocol (RIP) split-horizon is enabled on an interface that is configured with multiple IP addresses, a single update sourced by the primary IP address is sent advertising only the major networks. If split-horizon is disabled, multiple updates sourced from each address on the interface are sent and all subnets are advertised.

When configuring an Open Shortest Path First (OSPF) interface, use the **ip address** command first to establish the interface, and then enable OSPF on it by using the **interface-ospf** command in OSPF area configuration mode; see Chapter 33, "OSPF Commands." The primary IP address of the interface must belong to the area in which OSPF is enabled. In addition, only neighbors on the primary address subnet can be OSPF peers.

Caution Removing the primary IP address disables all IP services for that address on the specified interface. Disabling IP services deletes a corresponding OSPF interface from the running configuration.

To assign an IP address to a subscriber, use the **ip address** command in subscriber configuration mode; see Chapter 8, "Subscriber Commands."

Use the **no** form of this command to remove an IP address from an interface. You must remove all secondary IP addresses before you can remove the primary IP address.

Examples

The following commands assign an IP address and netmask to the interface named `enet1`:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip address 10.4.5.2 255.255.255.0
```

The following commands configure two noncontiguous CIDR blocks for the interface `Downstream`:

```
[local]RedBack(config)#context local
[local]RedBack(config)#interface Downstream
[local]RedBack(config)#ip address 10.0.0.1 255.255.255.0
[local]RedBack(config)#ip address 11.0.0.1 255.255.255.0 secondary
```

The following commands allow the circuit for subscriber `fred` to bind to the `Downstream` interface using either IP address:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#subscriber name fred
[local]RedBack(config-ip)#ip address 10.0.0.2 255.255.255.240
[local]RedBack(config-ip)#ip address 11.0.0.2 255.255.255.240
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#atm pvc 0 1 profile UBR encapsulation bridge1483
[local]RedBack(config-pvc)#bind subscriber fred@local
```

Related Commands

debug ip interface
ip pool
ip rip listen

ip secured-arp
network
ospf-interface
show ip interface

ip arp arpa

ip arp arpa

no ip arp arpa

Purpose

Enables the standard Ethernet Address Resolution Protocol (ARP) on an interface.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

ARP is disabled on all interfaces.

Usage Guidelines

Use the **ip arp arpa** command enable standard Ethernet ARP on the interface; see RFC 826, *An Ethernet Address Resolution Protocol*.

This command does not apply to loopback interfaces or to PPP default interfaces.

Use the **no** form of this command to disable ARP on the interface.

Examples

The following example sets the address resolution type for the interface named `enet1` to standard Ethernet ARP:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip arp arpa
```

Related Commands

debug ip interface
ip arp timeout
ip secured-arp
show ip arp
show ip interface

ip arp timeout

ip arp timeout *seconds*

no ip arp timeout

Purpose

Sets the number of seconds that an idle Address Resolution Protocol (ARP) entry remains in the system's cache table.

Command Mode

interface configuration

Syntax Description

seconds	Number of seconds before an ARP cache entry is aged out. The range of values is 10 to 4,294,967. The default value is 3,600.

Default

The default ARP cache timeout is 3,600 seconds (1 hour).

Usage Guidelines

Use the **ip arp timeout** command to modify the ARP cache timeout value.

This command does not apply to loopback or PPP default interfaces.

Use the **no** form of this command to restore the default timeout value of 3,600 seconds.

Examples

The following example sets the ARP cache timeout value to `7200` for the interface named `enet1`:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip arp timeout 7200
```

Related Commands

debug ip interface
ip arp arpa
ip secured-arp
show ip arp
show ip interface

ip ignore-df-bit

ip ignore-df-bit

{**no** | **default**} **ip ignore-df-bit**

Purpose

Allows a forwarded IP packet to be fragmented when its length exceeds the maximum transmission unit (MTU) size associated with the outgoing interface, regardless of the packet's "don't fragment" setting.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

When fragmentation is required to forward an IP packet and the packet's "don't fragment" bit is set, the outgoing interface discards the packet.

Usage Guidelines

Use the **ip ignore-df-bit** command to allow a forwarded IP packet to be fragmented when its length exceeds the MTU size associated with the outgoing interface, regardless of the packet's "don't fragment" setting.

Caution This command can have a serious impact on forwarding performance and behavior and should not be enabled except under the direction of Redback support personnel.

For details on this feature, see RFC 1191, *Path MTU Discovery* and RFC 2923, *TCP Problems with Path MTU Discovery.*

Use the **no** or **default** form of this command to return to the default behavior of discarding packets that have the "don't fragment" bit set and that exceed the MTU size associated with the outgoing interface.

Examples

The following example allows a forwarded IP packet to be fragmented when its length exceeds the MTU size of `1000` bytes for the outgoing interface `eth1`:

```
[local]RedBack(config-ctx)#interface eth1
[local]RedBack(config-if)#ip address 10.10.1.1 255.255.255.0
[local]RedBack(config-if)#ip mtu 1000
[local]RedBack(config-if)#ip ignore-df-bit
```

Related Commands

ip mtu

ip lookup host

ip lookup host

no ip lookup host

Purpose

Configures the SMS device to look at the host table first when selecting the next-hop interface for packets received on this interface.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

Routing table lookup is performed before host table lookup.

Usage Guidelines

Use the **ip lookup host** command to optimize the performance of an interface by looking at the host table, rather than the routing table, first when choosing the next-hop destination for packets received on this interface.

This command is helpful if the vast majority of packets received on an interface are destined for hosts that are likely to be directly attached because configuring the interface to look for the next-hop interface in the host table first can provide significant improvements in traffic throughput.

This command does not apply to loopback interfaces.

Use the **no** form of this command to set the SMS device to start the search for a next-hop destination in the routing table.

Examples

The following example enables host table lookup first for packets received by the interface named `enet1`:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip lookup host
```

Related Commands

debug ip interface
show ip interface

ip mask-reply

ip mask-reply

{**no** | **default**} **ip mask-reply**

Purpose

Enables an interface to send Internet Control Message Protocol (ICMP) mask replies on receipt of an ICMP mask request.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

The sending of ICMP mask replies is disabled.

Usage Guidelines

Use the **ip mask-reply** command to enable an interface to send an ICMP mask reply upon receipt of an ICMP mask request.

This command does not apply to loopback interfaces.

Use the **no** or **default** form of this command to disable the sending of ICMP mask replies.

Examples

The following example enables the sending of ICMP mask replies on the interface named `mgmt`:

```
[local]RedBack(config-ctx)#interface mgmt
[local]RedBack(config-if)#ip mask-reply
```

Related Commands

debug ip icmp
debug ip interface
ping
show ip interface

ip mtu

ip mtu *bytes*

no ip mtu *bytes*

Purpose

Sets the maximum transmission unit (MTU) size for IP packets sent on an interface.

Command Mode

interface configuration

Syntax Description

bytes	MTU size in bytes. The range of values is 48 to 9,216. The default is 1,500.

Default

The MTU size is 1,500 bytes.

Usage Guidelines

Use the **ip mtu** command to set the MTU size for IP packets sent on an interface. If an IP packet exceeds the MTU configured for an interface, the system fragments that packet.

This command does not apply to loopback interfaces.

Use the **no** form of this command to restore the default MTU size of 1,500 bytes.

Examples

The following example sets the maximum IP packet size for the interface named `atm1` to 300 bytes:

```
[local]RedBack(config-ctx)#interface atm1
[local]RedBack(config-if)#ip mtu 300
```

Related Commands

debug ip interface
show ip interface

ip pool

ip pool *ip-address netmask*

no ip pool *ip-address netmask*

Purpose

Assigns a range of IP addresses from a locally defined pool to an interface.

Command Mode

interface configuration

Syntax Description

ip-address	IP address of the IP pool.
netmask	Network mask for the associated IP address.

Default

The interface IP address is not assigned from a pool.

Usage Guidelines

Use the **ip pool** command to assign a range of IP addresses from a locally defined pool to an interface. A pool is derived by applying the *netmask* argument to the *ip-address* argument, thus obtaining the network portion of the address. The interface address, the interface all-zeroes address, and the interface broadcast address are automatically excluded if they overlap the pool.

You must configure the Remote Authentication Dial-In User Service (RADIUS) server to return the Framed-IP-Address attribute with a value of 255.255.255.254 for the **ip pool** command to take effect. This RADIUS attribute informs the Subscriber Management System (SMS) device that the interface's IP address will be assigned from a pool.

You can specify more than one pool on an interface. This command does not apply to loopback interfaces.

Use the **no** form of this command to remove an IP address pool.

Examples

The following example shows the pool being set up and assumes that the RADIUS server has been configured to return the Framed-IP-Address attribute with a value of 255.255.255.254:

```
[local]RedBack(config)#context isp.net
[local]RedBack(config-ctx)#aaa authentication subscriber radius
[local]RedBack(config-ctx)#interface downstream
[local]RedBack(config-if)#ip address 10.0.0.1 255.255.255.0
[local]RedBack(config-if)#ip pool 10.0.0.2 255.255.255.0
```

Related Commands

debug ip interface
ip address—interface configuration mode
show ip interface
show ip pool

ip secured-arp

ip secured-arp

no ip secured-arp

Purpose

Enables the secured Address Resolution Protocol (ARP) on an interface.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

Secured ARP is disabled.

Usage Guidelines

Use the **ip secured-arp** command to enable secured ARP on an interface. You must also enable IP ARP using the **ip arp arpa** command in interface configuration mode before any ARP processing can take place on an interface.

When secured ARP is enabled on an interface, the Subscriber Management System (SMS) device sends ARP requests out an interface to resolve only those Media Access Control (MAC) addresses that correspond to configured subscriber IP addresses. In addition, ARP requests are only answered when secured by configured subscriber IP addresses for the corresponding interface. ARP requests are never flooded by a system interface to multiple-bound circuits.

This command does not apply to loopback interfaces or to PPP default interfaces.

Use the **no** form of this command to disable secured ARP on the specified interface.

Examples

The following example enables secured ARP on an interface named `enet1`:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip arp arpa
[local]RedBack(config-if)#ip secured-arp
```

Related Commands

ip arp arpa
show ip secured-arp

ip source-address

ip source-address {**snmp** [**radius**] | **radius** [**snmp**]}

no ip source-address[**snmp**] [**radius**]

Purpose

Configures the interface's primary IP address as the source address for all Simple Network Management Protocol (SNMP) trap packets and Remote Authentication Dial-In User Service (RADIUS) packets that are sent from the context.

Command Mode

interface configuration

Syntax Description

snmp	Configures the interface as the source for all SNMP trap packets sent from the context in which the interface resides.
radius	Configures the interface as the source IP address for all RADIUS packets sent from the context in which the interface resides.

Usage Guidelines

Use the **ip source-address** command to configure the interface to be the source IP address for SNMP trap packets and RADIUS packets sent from the context. You can specify the **snmp** keyword, the **radius** keyword, or both. Use the **snmp** keyword to ensure that all SNMP trap packets issued from the context in which the interface resides use the interface's primary IP address as the source IP address for those packets, even if packets are sent out through another interface. Use the **radius** keyword to enable this functionality for RADIUS packets.

Use the **no** form of this command to disable IP source addressing.

Examples

The following example configures the interface at IP address `10.1.1.1` as the source IP address for SNMP trap packets:

```
[local]RedBack(config-if)#ip address 10.1.1.1
[local]RedBack(config-if)#ip source-address snmp
```

Related Commands

show ip interface

show ip arp

show ip arp [*ip-address*]

Purpose

Displays the IP Address Resolution Protocol (ARP) table for the current context.

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address for which IP ARP information is displayed.

Default

Displays all ARP table entries.

Usage Guidelines

Use the **show ip arp** command to display the IP ARP table for the current context. If the *ip-address* argument is not specified, the entire ARP cache is displayed. Otherwise, only the entry matching the specified IP address is displayed. This commands displays information on host address, next-hop count, MAC address, address resolution status, and time-to-live value information.

Note This command is also described in Chapter 8, "Subscriber Commands."

Examples

The following shows sample output from the **show ip arp** command:

```
[local]RedBack>show ip arp

Host            Nhop cct    Mac address        State     Ttl
10.53.7.10      30000001    00:60:97:a1:5a:a3  resolved  2939
10.53.7.11      30000001    00:a0:24:dd:a4:46  resolved  3253
10.53.7.14      30000001    00:a0:24:c8:92:9f  resolved  3395
10.53.7.17      30000001    00:a0:24:bf:8c:5c  resolved  2883
10.53.7.18      30000001    00:00:a0:0b:04:07  resolved  3145
10.53.7.20      30000001    00:a0:24:bf:8c:13  resolved  3293
10.53.7.36      30000001    00:60:08:02:96:20  resolved  3337
```

Related Commands

ip arp arpa

show ip interface

show ip interface [**brief** | *if-name* [**access-statistics**]]

Purpose

Displays information about IP interfaces configured in the current context.

Command Mode

operator exec

Syntax Description

brief	Optional. Displays summary information about all interfaces configured in the current context.
if-name	Optional. Name of the interface for which information is displayed.
access-statistics	Optional. Displays the number of inbound and outbound packets filtered by the access list configured on the particular interface.

Default

Displays all IP interfaces in the current context.

Usage Guidelines

Use the **show ip interface** command to display information about IP interfaces configured in the current context. When the *if-name* argument is not specified, this command displays information about all interfaces configured in the current context. When the *if-name* argument is provided, additional information is displayed about the specified interface, including a list of all circuits or ports currently bound to that interface and their state. The **brief** keyword displays summary information about all interfaces configured in the context.

The **access-statistics** keyword displays the number of inbound and outbound packets filtered by the access control list configured on the particular interface.

An interface is only in the up state if at least one underlying circuit on an operational port is bound to it. All higher-layer protocols, such as the Routing Information Protocol (RIP), are not enabled on an interface that is shut down.

Examples

The following example shows information about the configured interfaces:

```
[local]RedBack>show ip interface

Intf name:      enet0
IP state:       Up                  Cost:           0
IP address:     10.1.1.1            Subnet mask:    255.255.255.0
Bcast address:  10.1.1.255          MTU:            1500
Lookup method:  Host First          Intf index:     1
Resoln type:    Arp                 ARP timeout:    3600
Secured ARP:    Disabled            ICMP mask repl: Disabled
Access Control: Off                 IGMP Proxy:     Disabled
PPP-Proxy ARP:  Disabled            Interface type: Standard
IRDP:           Disabled

Intf name:      atm00
IP state:       Up                  Cost:           0
IP address:     20.1.1.1            Subnet mask:    255.255.255.0
Bcast address:  20.1.1.255          MTU:            1500
Lookup method:  Route First         Intf index:     3
Resoln type:    None                ARP timeout:    3600
Secured ARP:    Disabled            ICMP mask repl: Disabled
Access Control: Off                 IGMP Proxy:     Disabled
PPP-Proxy ARP:  Disabled            Interface type: Standard
IRDP:           Disabled
```

The following example shows use of the **access-statistics** keyword:

```
[blue]RedBack>show ip interface eth2 access-statistics

Intf name:      eth2
IP state:       Dormant             Cost:           0
IP address:     10.20.30.40         Subnet mask:    255.255.255.0
Bcast address:  10.20.30.255        MTU:            1500
Lookup method:  Route First         Intf index:     0
Resoln type:    None                ARP timeout:    3600
Secured ARP:    Disabled            ICMP mask repl:  Disabled
Access Control: On                  IGMP proxy:     Disabled
PPP-Proxy ARP:  Disabled            Intf type:     Standard
IRDP:           Disabled

Bindings:
slot/port       ethernet type       state    source-validation
3/1             ethernet Explicit   Down     Off

Outbound IP access-statistics:
    permit      =      0        deny        =    0
    redir       =      0        bad redir   =
```

Related Commands

format
interface
ip address
ip igmp
ip lookup host
ip mask-reply
ip mtu
ip pool
ip rip interface-cost
ip rip listen
ip rip receive version
ip rip send version
ip secured-arp
network
ospf-interface

show ip pool

show ip pool

Purpose

Displays all IP address pools for the current context.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show ip pool** command to display all IP pools for the current context. A list of IP addresses from pools assigned to interfaces are displayed, as are the number of addresses in use, available, or unusable. Unusable addresses include those used by an interface or the interface's all ones or all zeros address.

Examples

The following example displays output from the **show ip pool** command:

```
[local]RedBack>show ip pool

Interface "cool":
     1.1.1.0       255.255.255.248  0 in use,   6 free,  2 unusable.
     1.1.1.32      255.255.255.248  0 in use,   8 free,  0 unusable.
     1.1.1.248     255.255.255.248  0 in use,   7 free,  1 unusable.
Interface "hot":
     10.1.1.0      255.255.255.0    0 in use, 253 free,  3 unusable.
```

Related Commands

ip pool
ip address—interface configuration mode

show ip secured-arp

show ip secured-arp [*ip-address*]

Purpose

Displays IP hosts residing on network segments associated with interfaces in the current context for which secured Address Resolution Protocol (ARP) is enabled

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address of a specific host.

Default

Displays all secured ARP table entries.

Usage Guidelines

Use the **show ip secured-arp** command to display information about IP hosts that reside on network segments associated with secured ARP interfaces in the current context. If the *ip-address* argument is not specified, the entire secured ARP table is displayed; otherwise, only the entry matching the specified IP address is displayed.

Examples

The following example displays all secured ARP table entries:

```
[local]RedBack>show ip secured-arp

Host         Nhop cct    Interface

10.1.1.2     18000010    1
20.1.1.2     18010011    2
30.1.1.2     18020012    3
40.1.1.2     18030013    4
```

Related Commands

ip secured-arp

Subscriber Commands

This chapter describes the commands used to configure, maintain, and troubleshoot subscribers and subscriber sessions through the Access Operating System (AOS).

Note For protocol-specific, or feature-specific, subscriber configuration mode commands, see the appropriate chapter in this guide. For example, to enable subscribers to transmit or receive IP multicast traffic, see Chapter 36, "IGMP Proxy Commands."

For overview information, a description of the tasks used to configure subscribers, and configuration examples, see the "Configuring Subscribers" chapter in the *Access Operating System (AOS) Configuration Guide*.

clear arp-cache

clear arp-cache [*host-address*]

Purpose

Removes one or all entries from the dynamic Address Resolution Protocol (ARP) cache in the current context.

Command Mode

administrator exec

Syntax Description

host-address	Optional. IP address of host to remove from ARP cache, in the form *A.B.C.D*.

Default

Clears all entries in the ARP cache.

Usage Guidelines

Use the **clear arp-cache** command to remove erroneous or outdated information in the ARP cache for the current context. If you do not specify the *host-address* argument, all entries in the ARP cache are cleared. Otherwise, only entry matching the *host-address* argument is cleared.

Examples

The following example clears the entire ARP cache:

```
[local]RedBack#clear arp-cache
```

The following example clears only the host at IP address `10.1.1.1` from the ARP cache:

```
[local]RedBack#clear arp-cache 10.1.1.1
```

Related Commands

show ip arp
show ip host

clear subscriber

clear subscriber *subscriber*

Purpose

Clears the subscriber.

Command Mode

operator exec

Syntax Description

subscriber	Name of the subscriber to be cleared, in any valid structured username format.

Default

None

Usage Guidelines

Use the **clear subscriber** command to disconnect a subscriber session. The Access Operating System (AOS) verifies whether the subscriber is currently active and, if so, clears the circuit to which the subscriber is bound. In the case of the Point-to-Point Protocol (PPP), the PPP state machine terminates the session, and logs the subscriber out. It then attempts to renegotiate and reauthenticate a new session with the remote peer on that circuit. In the case of RFC 1483-encapsulated and RFC 1490-encapsulated circuits, the circuit is brought down and then back up, and an attempt is made to reauthenticate the subscriber that is bound to that circuit.

This command is useful when a subscriber's record has changed and you want the new parameters to take effect immediately. It is also useful when a user account has been removed and you want to log the user off.

Note This command is also described in Chapter 42, "System Monitoring and Testing Commands."

Examples

The following example clears the subscriber `dave@isp1`:

```
[local]RedBack>clear subscriber dave@isp1
```

Related Commands

show subscribers

debug ip arp

debug ip arp

no debug ip arp

Purpose

Enables the logging of IP Address Resolution Protocol (ARP) debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip arp** command to enable the logging of IP ARP-related messages. You can use the **logging console** and **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Examples

The following example enables the logging of IP ARP-related messages:

```
[local]RedBack#debug ip arp
```

Related Commands

ip arp
logging console
show ip arp
terminal monitor

ip address

ip address {*ip-address* [*netmask*] | **pool** [**name** *if-name*]}

no ip address {*ip-address* [*netmask*] | **pool** [**name** *if-name*]}

Purpose

Configures the IP address of the subscriber's circuit.

Command Mode

subscriber configuration

Syntax Description

ip-address	IP address of the subscriber's circuit.
netmask	Optional. Specifies the network mask for the IP address. You must enter a mask of at least 24 bits; that is, a mask in the range 255.255.255.0 to 255.255.255.255.
pool	Optional. Indicates that the subscriber's circuit is assigned an IP address from a locally-managed IP address pool.
name *if-name*	Optional. Assigns the subscriber's address from the IP address pool configured for the specified interface.

Default

None

Usage Guidelines

Use the **ip address** command to configure the IP address of the subscriber's circuit. To specify a range of contiguous IP addresses, use the optional *netmask* argument. For Point-to-Point Protocol (PPP)-encapsulated circuits, only the first IP address in a subscriber record is used for address negotiation. For subscriber circuits using RFC 1483 encapsulation or RFC 1490 encapsulation, entries are added to the host table for any and all such IP addresses.

You can specify either an IP address or an IP pool, but not both. When using the **pool** keyword, you must ensure that the Remote Authentication Dial-In Service (RADIUS) server is configured to return the correct value for the Framed_IP_Address attribute (255.255.255.254). Any IP address assigned to a subscriber must fall within the address and netmask range configured for an interface in the context to which the subscriber is to be bound; otherwise, the binding will fail. The same is true of IP addresses returned by RADIUS servers that are to be assigned to subscribers.

The **name** *if-name* construct specifies that the subscriber's address is to be assigned from the address pool configured for that interface. In this case, the Access Operating System (AOS) is prohibited from selecting an IP address pool other than the one specified. If there are no remaining addresses in the pool maintained for the named interface, the subscriber's PPP session fails.

If there is more than one host attached, use the **ip host** command in circuit configuration mode in succession to configure multiple IP addresses.

Use the **no** form of this command to remove an IP address from a subscriber record.

To assign an address to an interface, use the **ip address** command in interface configuration mode; see Chapter 7, "Interface Commands."

Example

The following example defines the IP address `10.1.1.7` for a subscriber named `host1`:

```
[local]RedBack(config-ctx)#subscriber name host1
[local]RedBack(config-sub)#ip address 10.1.1.7
```

The next example defines two IP addresses, `10.1.1.14` and `10.1.1.15`, for a subscriber named `host2`:

```
[local]RedBack(config-ctx)#subscriber name host2
[local]RedBack(config-sub)#ip address 10.1.1.14
[local]RedBack(config-sub)#ip address 10.1.1.15
```

The following example defines eight IP addresses, `10.1.1.32` through `10.1.1.39`, for a subscriber named `host8`:

```
[local]RedBack(config-ctx)#subscriber name host8
[local]RedBack(config-sub)#ip address 10.1.1.32 255.255.255.248
```

In the next example, the subscriber `joe` will always be assigned an address in the range 1.1.1.x, if one is available. If one is not available, the session for subscriber `joe` will fail.

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface If_One
[local]RedBack(config-if)#ip address 1.1.1.1 255.255.255.0
[local]RedBack(config-if)#ip pool 1.1.1.2 255.255.255.0
[local]RedBack(config-if)#interface If_Two
[local]RedBack(config-if)#ip address 2.2.2.2 255.255.255.0
[local]RedBack(config-if)#ip pool 2.2.2.2 255.255.255.0
[local]RedBack(config-if)#subscriber name joe
[local]RedBack(config-sub)#ip address pool name If_One
```

Related Commands

bind subscriber
ip host—circuit configuration mode
ip pool
show subscribers

ip arp

ip arp *ip-address mac-address*

no ip arp *ip-address mac-address*

Purpose

Creates an entry in the Address Resolution Protocol (ARP) cache for a subscriber whose host is not capable of (or is not configured to) responding to ARP requests.

Command Mode

subscriber configuration

Syntax Description

ip-address	IP address of the subscriber's host.
mac-address	Media Access Control (MAC) address of the subscriber's host.

Default

None

Usage Guidelines

Use the **ip arp** command to create an entry in the ARP cache for a subscriber whose host is not capable (or is not configured to) respond to ARP requests. This command is only relevant on circuits using RFC 1483 bridged encapsulation or RFC 1490 bridged encapsulation. This command is available for individual subscriber records, but not for a default subscriber record.

Use the **no** form of this command to remove the specified entry from the system's configuration and to prevent the entry from being created in the ARP cache.

Examples

The following example configures an ARP cache entry for a host with IP address `10.1.1.1` and hardware address `d3:9f:23:46:77:13` for a subscriber named `NoGrokARPs`. The entry will be installed into the ARP cache of the appropriate interface when the circuit is brought up.

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#subscriber name NoGrokARPs
[local]RedBack(config-sub)#ip address 10.1.1.1
[local]RedBack(config-sub)#ip arp 10.1.1.1 d3:9f:23:46:77:13
```

Related Commands

debug ip arp
show ip arp

ip source-validation

ip source-validation

no ip source-validation

Purpose

Enables IP source-address validation.

Command Mode

subscriber configuration

Syntax Description

There are no keywords or arguments for this command.

Default

IP source-address validation is disabled.

Usage Guidelines

Use the **ip source-validation** command to enable IP source-address validation. IP source address validation, also known as ingress filtering, denies all IP packets from address sources that are not reachable through the subscriber's associated circuit. You can use this command to prevent address spoofing.

Enabling this feature can cause a significant increase in Forwarding Engine (FE) memory consumption and performance degradation. The administrator should be certain that this feature is required before enabling it.

Use the **no** form of this command to disable IP source-address validation.

Examples

The following example enables IP source-address validation for the subscriber named `bart`:

```
[local]RedBack(config-ctx)#subscriber name bart
[local]RedBack(config-sub)#ip source-validation
```

Related Commands

show subscribers

ip tos-field

ip tos-field {**normal** | **min-cost** | **max-reliability** | **max-throughput** | **min-delay** | **raw** *value*}

no ip tos-field

Purpose

Statically resets the type of service (ToS) bit on all session traffic.

Command Mode

subscriber configuration

Syntax Description

normal	Sets the ToS to normal operation.
min-cost	Sets the ToS to minimize monetary cost.
max-reliability	Sets the ToS to maximize reliability.
max-throughput	Sets the ToS to maximize throughput.
min-delay	Sets the ToS to minimize delay.
raw *value*	Hexadecimal digit, preceded with the characters ‘0x’. The bit values are as follows: • no bits=Normal (0) • bit 1=Minimum Cost (1) • bit 2=Maximum Reliability (2) • bit 3=Maximum Throughput (4) • bit 4=Minimum Delay (8) A value can indicate one or more ToS bit values. To specify more than one type of service, add the value for each desired ToS, and specify the sum total as the value. The maximum bit value is the total of all bit values (0+1+2+4+8=15).

Default

The ToS bit is not reset and remains as it is received in the header of the incoming IP packet.

Usage Guidelines

Use the **ip tos-field** command to reset the ToS bit on all session traffic.

Use the **no** form of this command to return the system to its default behavior of not reset the ToS bit.

Examples

The following example specifies two types of service—the maximum throughput (value of 4) and maximum reliability (value of 2), producing a sum total value of 6:

```
[local]Redback(config-sub)#ip tos-field raw 0x6
```

The following example resets the ToS on incoming IP packets to maximize reliability:

```
[local]RedBack(config-sub)#ip tos-field max-reliability
```

Related Commands

show subscribers

outbound password

outbound password *password*

no outbound password

Purpose

Configures the password supplied by the Access Operating System (AOS) to the subscriber's host in order to authenticate the subscriber for a Point-to-Point Protocol (PPP) session.

Command Mode

subscriber configuration

Syntax Description

password	Alphanumeric text string. Control characters are not allowed.

Default

None

Usage Guidelines

Use the **outbound password** command to configure the password supplied during Challenge Handshake Authentication Protocol (CHAP)/Password Authentication Protocol (PAP) authentication. You can enter a password with embedded spaces by enclosing the entire password in double quotes; for example, "This is a Password With Spaces."

Use the **no** form of this command to remove the password from the subscriber's record.

Examples

The following example configures an outbound password of `DontTellAnyone`:

```
[local]RedBack(config-sub)#outbound password DontTellAnyone
```

Related Commands

password

password

password *password*

no password

Purpose

Configures the authentication password that the subscriber enters when initiating a Point-to-Point Protocol (PPP) session.

Command Mode

subscriber configuration

Syntax Description

password	Alphanumeric text string. Control characters are not allowed.

Default

None

Usage Guidelines

Use the **password** command to configure the authentication password that the subscriber enters when initiating a PPP session. When using Challenge Handshake Authentication Protocol (CHAP)/Password Authentication Protocol (PAP), the password obtained from the subscriber must match the password configured in the corresponding subscriber record. This command is available for individual subscriber records, but not for a default subscriber record.

You can enter a password with embedded spaces by enclosing the entire password in double quotes; for example, “This is a Password With Spaces.”

Use the **no** form of this command to remove the password from the subscriber’s record.

Examples

The following example configures a password of `DontTellAnyone`:

```
[local]RedBack(config-sub)#password DontTellAnyone
```

Related Commands

outbound password

police

police rate *rate* **burst** *size*

no police

Purpose

Specifies the rate and burst tolerance of traffic received on a subscriber's circuit.

Command Mode

subscriber configuration

Syntax Description

rate *rate*	Rate in kbps. The range of values is 10 to 155,520.
burst *size*	Burst tolerance in bytes. The range of values is 0 to 100,000.

Default

Policing is disabled.

Usage Guidelines

Use the **police** command to specify the rate and burst tolerance of traffic received on a subscriber's circuit. This command limits the aggregate packet stream to the specified rate and burst tolerance. Packets exceeding the specified rate and burst tolerance are dropped. A typical burst tolerance is ten times the link maximum transmission unit (MTU), or approximately 15,000 to 20,000 bytes. A larger burst tolerance is generally appropriate for backhaul circuits.

Use the **no** form of this command to remove the policing feature from the subscriber's record.

Examples

The following example sets the rate to `200` kbps and the burst tolerance to `15000` bytes:

```
[local]RedBack(config-sub)#police rate 200 burst 15000
```

Related Commands

rate-limit—subscriber configuration mode

port-limit

port-limit *max-sessions*

no port-limit

Purpose

Limits the number of sessions a subscriber can access simultaneously.

Command Mode

subscriber configuration

Default

There are no session limits.

Syntax Description

max-sessions	Maximum number of simultaneous subscriber sessions allowed. The range of values is 1 to 255.

Usage Guidelines

Use the **port-limit** command to limit the number of sessions a subscriber can access simultaneously. This command is useful for dialup and Integrated Services Digital Network (ISDN) users who might attempt to consume more than two links in their multilink bundle. You can also use this command to prevent a single user's account from being accessed by multiple users.

To set the port limit remotely via RADIUS, use the Port-Limit RADIUS attribute described in the "RADIUS Attributes" appendix in the *Access Operating System (AOS) Configuration Guide*.

Note This command is also described in Chapter 23, "PPP and PPPoE Commands."

Examples

The following example sets a maximum of 2 links for subscriber `joe` to use simultaneously:

```
[local]RedBack(config)#subscriber name joe
[local]RedBack(config-subscriber)#port-limit 2
```

Related Commands

show subscribers

rate-limit

rate-limit rate *rate* **burst** *size*

no rate-limit

Purpose

Specifies the rate and burst tolerance of traffic sent on a subscriber's circuit.

Command Mode

subscriber configuration

Syntax Description

rate *rate*	Rate in kbps. The range of values is 10 to 155,520.
burst *size*	Burst tolerance in bytes. The range of values is 0 to 100,000.

Default

Rate limiting is disabled.

Usage Guidelines

Use the **rate-limit** command to limit the aggregate packet stream transmitted on a subscriber's circuit, Point-to-Point Protocol (PPP) session, or PPP over Ethernet (PPPoE) session to the specified rate and burst tolerance. Packets exceeding the specified rate and tolerance are dropped.

A reasonable rule-of-thumb for burst tolerance is 10 times the link maximum transmission unit (MTU), or approximately 15,000 to 20,000 bytes. A larger burst tolerance is generally appropriate for backhaul circuits.

Use the **no** form of this command to disable the rate-limiting feature from the subscriber's record.

Examples

The following example sets the rate to `100000` kbps and the burst tolerance to `15000` bytes:

```
[local]RedBack(config-sub)#rate-limit rate 100000 burst 15000
```

Related Commands

police—subscriber configuration mode

show ip arp

show ip arp [*ip-address*]

Purpose

Displays the IP Address Resolution Protocol (ARP) table for the current context.

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address of the ARP table entry to display, in the form *A.B.C.D*.

Default

Displays all ARP table entries.

Usage Guidelines

Use the **show ip arp** command to display the IP ARP table for the current context. If the *ip-address* argument is not specified, the entire ARP cache is displayed. Otherwise, only the ARP cache entry matching the argument address is displayed.

Note This command is also described in Chapter 7, "Interface Commands."

Examples

The following example displays sample output from the **show ip arp** command:

```
[local]RedBack>show ip arp

Host            Nhop cct    Mac address        State     Ttl
10.53.7.10      30000001    00:60:97:a1:5a:a3  resolved  2939
10.53.7.11      30000001    00:a0:24:dd:a4:46  resolved  3253
10.53.7.14      30000001    00:a0:24:c8:92:9f  resolved  3395
10.53.7.17      30000001    00:a0:24:bf:8c:5c  resolved  2883
10.53.7.18      30000001    00:00:a0:0b:04:07  resolved  3145
10.53.7.20      30000001    00:a0:24:bf:8c:13  resolved  3293
10.53.7.36      30000001    00:60:08:02:96:20  resolved  3337
```

Related Commands

debug ip arp
ip arp

show subscribers

show subscribers [**access-statistics** [*sub-name*] | **active** [*sub-name*] | **address** *sub-name* | **all** | **minimums** [*ctx-name* | **all**] | **summary**]

Purpose

Displays subscriber information.

Command Mode

operator exec

Syntax Description

access-statistics *sub-name*	Optional. Displays the number of incoming and outgoing packets filtered by the access control list. If you do not specify the *sub-name* argument, access statistics are displayed for all subscribers in the context. If you specify the *sub-name* argument, only access statistics for that subscriber are displayed.
active *sub-name*	Optional. Displays a list of active users.
address *sub-name*	Optional. Displays IP addresses currently in use by the specified subscriber.
all	Optional. Displays information for subscribers in all contexts. This option is available only to operators and administrators in the local context.
minimums *ctx-name* | **all**	Optional. When you do not specify the *ctx-name* argument, displays reserved subscriber slots for the current context. When you specify the *ctx-name* argument, displays reserved subscriber slots for that context. When you specify the **all** keyword, reserved subscriber slots for all contexts are displayed. The **all** keyword is available only when the current context is local.
summary	Optional. Displays a summary of subscriber information.

Default

Displays information for all active subscribers in the current context.

Usage Guidelines

Use the **show subscribers** command to display subscriber information.

You must specify the **access-statistics** keyword in the context in which the subscriber whose information is being queried is configured.

When you use the **address** keyword, nothing is displayed if the subscriber is currently not logged on or has no IP addresses. This command will display all addresses for RFC 1483-encapsulated or RFC 1490-encapsulated subscriber circuits and for Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE) subscribers. It displays Dynamic Host Configuration Protocol (DHCP)-assigned addresses and authentication, authorization, and accounting (AAA)-assigned addresses.

Use the **minimums** keyword to display, at the context and tunnel peer level, the minimum number of subscriber slots reserved in the current context. If the current context is local, you have additional options of displaying reserved minimums for a specific context or for all contexts. Set reserved subscriber minimums using either the **aaa min-subscribers** command (context-level reservation) or the **l2x profile** and **profile** commands (tunnel peer-level reservation).

The **summary** keyword omits per-subscriber information and prints only the total number of subscribers and their encapsulations. A subscriber name appears in the table whenever the corresponding link is up.

Note This command is also described in Chapter 42, “System Monitoring and Testing Commands.”

Examples

The following example demonstrates the default information provided by the **show subscribers** command:

```
[local]RedBack>show subscribers

 CIRCUIT      SUBSCRIBER        CONTEXT   START TIME
 ---------------------------------------------------------------------
 PPPOE 00001   pppoe@redback.com  redback.com FRI DEC 04 17:46:49 1998
 ---------------------------------------------------------------------
 Total = 1 (ppp = 1, r-1483 = 0, b-1483 = 0, r-1490 = 0, b-1490 = 0)

[local]RedBack>show subscribers address pppoe

Host            Nhop cct    Interface
155.53.196.2    7000001     pool
```

The following example demonstrates the use of the **access-statistics** keyword:

```
[local]RedBack>show subscribers access-statistics

Subscriber name: atm501@local
Inbound IP access-statistics:
permit = 0 deny = 0
redir = 0 bad redir = 0
```

The following example shows using the **show subscribers minimums** command in the `local` context to display reserved subscriber minimums in all contexts.

Note When the word `Implied` appears in parentheses in the output, it means that the subscriber slots are reserved at the tunnel peer level as opposed to being reserved at the context level. The reservation at the context level is, therefore, implied.

```
[local]RedBack>show subscriber minimums all

Total subscribers in the system: 4000

CONTEXT      TUNNEL    MIN. SUB(Context)  MIN. SUB(Tunnel)  OCCUPIED
=====================================================================
             gentle                        200               0
local                  200 (Implied)
---------------------------------------------------------------------
              ben                          10                0
tribune                10 (Implied)
---------------------------------------------------------------------
Total                  210                                  0

Unreserved slots: 3790
Currently occupied unreserved slots: 0
```

The following example shows using the **show subscribers minimums** command in the `local` context to display reserved subscriber minimums for the context called `tribune`:

```
[local]RedBack>show subscriber minimums tribune

Minimum Subscribers (Implied):  10

TUNNEL PROFILE        MIN. SUBSCRIBERS        OCCUPIED
=======================================================
ben                   10                      0
```

Related Commands

aaa min-subscribers
bridge-group
clear circuit
clear subscriber
interface
ip access-group—subscriber configuration mode
ip address—subscriber configuration mode
show bindings
show ppp
subscriber

subscriber

subscriber {**default** | **name** *name*}

no subscriber {**default** | **name** *sub-name*}

Purpose

Configures a default or individual subscriber record and enters subscriber configuration mode.

Command Mode

context configuration

Syntax Description

default	Specifies the default subscriber record.
name *name*	Identifies an individual subscriber record.

Default

None

Usage Guidelines

Use the **subscriber** command to configure a default or individual subscriber record.

Use the **default** keyword to create a special subscriber record. Each configured attribute of the **default** subscriber is appended to all subscriber records in the context. However, if you configure a particular attribute, or set of attributes with a different value in an individual subscriber record, the value set in the individual subscriber record overrides the value set in the default subscriber record. This is true whether the individual subscriber record is created through local configuration or is accessed through a Remote Authentication Dial In User Service (RADIUS) server.

Use the **name** *name* construct to configure an individual subscriber record.

Use the **no** form of this command to remove a subscriber record.

Examples

The following example creates the subscriber named `dave`:

```
[local]RedBack(config-ctx)#subscriber name dave
[local]RedBack(config-sub)#
```

The following example configures primary and secondary Domain Name System (DNS) servers for the default subscriber record:

```
[local]RedBack(config-ctx)#subscriber default
[local]RedBack(config-sub)#dns primary 10.1.1.1
[local]RedBack(config-sub)#dns secondary 10.1.1.2
```

Related Commands

aaa authentication subscriber
bind authentication
bind subscriber
show subscribers

timeout

timeout {**absolute** | **idle**} *minutes*

{**default** | **no**} **timeout**

Purpose

Sets an idle or absolute Point-to-Point Protocol (PPP) or PPP over Ethernet (PPPoE) timeout for a subscriber.

Command Mode

subscriber configuration

Syntax Description

absolute	Specifies an absolute timeout after which the subscriber is disconnected from the session.
idle	Specifies an idle timeout. This is the amount of time allowed for no activity by the subscriber before the session is dropped.
minutes	Time, in minutes, that will elapse before a timeout occurs. The range of values is 10 to 596,523.

Default

No timeout is defined.

Usage Guidelines

Use the **timeout** command to set the time after which a subscriber's session is dropped. You must first configure counters for Asynchronous Transfer Mode (ATM) and Frame Relay circuits for the **timeout** command to function. Use the **counters** command in ATM profile configuration mode or in Frame Relay profile configuration mode.

Use the **no** and **default** forms of this command to remove a timeout.

Examples

The following example sets an absolute timeout of `20` minutes:

```
[local]RedBack(config-sub)#timeout absolute 20
```

Related Commands

counters—ATM profile configuration mode
counters—Frame Relay profile configuration mode

Part 3

Ports, Circuits, Channels, and Bindings

Common Port, Circuit, and Channel Commands

This chapter describes the commands used to manage ports, circuits, and channels under the Access Operating System (AOS).

The commands described in this chapter are common across all port types, circuits, and channels, except where noted. Commands that are specific to a particular port type are described in the individual port chapters in this part of the book.

For overview information, a description of the tasks used to configure ports, channels, and circuits, and configuration examples, see the "Configuring Common Port, Circuit, and Channel Parameters" chapter in the *Access Operating System (AOS) Configuration Guide*.

buffers

buffers {**transmit** *value1* | **receive** *value2*}

default buffers {**transmit** | **receive**}

Purpose

Limits the total number of packet buffers that can be consumed by any one port.

Command Mode

port configuration

Syntax Description

transmit *value1*	Transmit queue size in number of packets. For all Asynchronous Transfer Mode (ATM) ports, the range of values is 1 to 4032; the default value is 256. For channelized DS-3 ports, the range of values is 1 to 992; the default is 64. For all other ports, the range of values is 10 to 1000; the default is 200.
receive *value2*	Receive queue size in number of packets. For all ATM ports, the range of values is 1 to 992; the default value is 192. For channelized DS-3 ports, the range of values is 1 to 992; the default is 64. For all other ports, the range of values is 10 to 1000; the default is 200.

Default

For all ATM ports, the default is 256 packet buffers for transmit, and 192 for receive. For channelized DS-3 ports, the default is 64 packet buffers for transmit and 64 for receive. For all other port types, the default is 200 packet buffers for transmit and 200 for receive.

Usage Guidelines

Use the **buffers** command to configure the number of receive or transmit buffers can be used for a port. When applied to a port, this command controls the sum of the transmit queues, or receive queues, for all circuits on that port.

Caution This command should be used with caution. Improperly setting this value can severely impact overall system performance. Consult with your technical support representative prior to modifying the default settings.

You can also configure the number of transmit buffers for ATM and Frame Relay circuits. See the **buffers** ATM profile configuration and Frame Relay configuration commands.

Use the **default** form of this command to return the number of buffers back to the default value.

Examples

The following example limits the transmit buffer size to `100` packets for port `0` in slot `3`:

```
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#buffers transmit 100
```

Related Commands

buffers—ATM profile configuration mode
buffers—Frame Relay profile configuration mode
show port info

bulkstats schema

bulkstats schema *schema-name* **format** *format-string* [*AOS-variable* [*AOS-variable* ...]]

no bulkstats schema *schema-name*

Purpose

Defines the port or High-level Data Link Control (HDLC) channel schema for the contents of the bulkstats collection file.

Command Mode

HDLC channel configuration
port configuration

Syntax Description

schema-name	Name of the schema. Can be no more than 19 characters in length.
format *format-string*	String used to format the output of the schema. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. Table 9-1 lists the supported special-character sequences.
AOS-variable	Optional. Variables for which data is collected. Separate the variables with a space. Table 9-2 lists the Access Operating System (AOS) variables available in port configuration mode.

Table 9-1 C Programming Language printf() Syntax

Syntax	Description
%s	A character string
%d	An integer in decimal (base 10)
%u	An unsigned integer in decimal (base 10)
%x	An integer in hexadecimal format (base 16)
%%	Gets replaced by a single % character in the output
\n	UNIX newline character

Table 9-2 AOS Variables

AOS Variable	Type	Description
slot	Integer	System slot number
port	Integer	Port number on the I/O module
description	String	Description of port
sysuptime	Integer	System uptime in seconds
inoctets	Integer	Number of octets received on this circuit
outoctets	Integer	Number of octets sent from this circuit
inpackets	Integer	Number of packets received on this circuit
outpackets	Integer	Number of packets sent on this circuit
mcast_inoctets	Integer	Number of multicast octets received on this circuit
mcast_outoctets	Integer	Number of multicast octets sent on this circuit
mcast_inpackets	Integer	Number of multicast packets received on this circuit
mcast_outpackets	Integer	Number of multicast packets sent on this circuit

Default

No schema is defined.

Usage Guidelines

Use the **bulkstats schema** command to define the port or HDLC channel schema for the contents of the bulkstats collection file. Schema names have an enforced maximum length of 19 characters.

You can configure multiple schemas, each gathering different data and formatting it differently for display. However, you should restrict the use of multiple schemas to global data collection and create only one schema per port, circuit, or profile. Otherwise, you can apply a profile with several schemas to a large number of circuits, slowing down the system processor function.

If you want to generate multiple collections of bulk statistics for a single port, circuit, or profile, create one schema designed to record separate groups of distinct data (subschemas) using the **\n** character sequence after each subset entry to create a new starting line.

When multiple schemas are defined in a configuration mode, each of the schemas is used to create a text record that is appended to the bulkstats collection file each sample period. Every line created always has the same schema name as the first field and has a new line appended as a record separator.

Use the **no** form of this command to delete the named bulkstats schema.

Examples

The following example creates a schema named `sample`:

```
[local]RedBack(config-port)#bulkstats schema sample format "global:%u,%u,%u, host:%s"
sysuptime date timeofday hostname
```

The result of the previous schema is formatted as follows:

```
sample: global: 348765, 19980924, 230834, host: isp1
```

Related Commands

bulkstats collection
bulkstats schema—ATM profile configuration mode
bulkstats schema—Frame Relay profile configuration mode

clear circuit

clear circuit {*slot/port* {*vpi vci* [**through** *end-vci*] | [*hdlc-channel*] *dlci* [**through** *end-dlci*] | **all**} | **pppoe** {[*cm-slot*-]*session-id* [**through** *end-session-id*] | **all**}}

Purpose

Clears active subscriber sessions on the specified circuits.

Command Mode

operator exec

Syntax Description

slot/port	Backplane slot number and port number of an Asynchronous Transfer Mode (ATM) or Frame Relay port.
vpi	Virtual path identifier (VPI) of the circuit. The range of values is 0 to 255.
vci	Virtual channel identifier (VCI) of the circuit. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when clearing a range of ATM circuits.
hdlc-channel	Name of the High-level Data Link Control (HDLC) channel in the case for a channelized DS-3 port. This argument is required for channelized DS-3 ports and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) of a configured Frame Relay permanent virtual circuit (PVC). The range of values is 16 to 991.
through *end-dlci*	Optional. Last DLCI when clearing a range of Frame Relay circuits.
pppoe [*cm-slot*-] *session-id*	Point-to-Point Protocol over Ethernet (PPPoE) session ID. The *cm-slot* argument is required for Connection Manager (CM) modules on the SMS 10000 device and is not used in any other case. It specifies the CM slot number. The *session-id* argument must be specified for all product platforms; the range of values is 1 to 65,535.
through *end-session-id*	Optional. Last session ID when clearing a range of PPPoE sessions.
all	With the *slot/port* argument, specifies that all circuits on the specified slot and port are cleared. With the **pppoe** keyword, specifies that all PPPoE sessions are cleared.

Default

None

Usage Guidelines

Use the **clear circuit** command to clear active subscriber sessions on the specified circuit or circuits. This command is similar to the **clear subscriber** command; instead of specifying the username, you specify the circuit or PPPoE session ID. This is particularly useful when a subscriber may be using multiple circuits and there is only one that you want to clear.

Once circuits are cleared using this command, they remain in the unconfigured state until new activity is detected on them. At that time, the configuration is read from Remote Authentication Dial-In User Service (RADIUS) or from the default circuit specification, if one is configured. If any configuration changes were made, they are implemented at that time.

Note This command is also described in Chapter 42, "System Monitoring and Testing Commands."

Examples

The following example clears all active subscriber sessions on all circuits on slot/port `3/0`:

```
[local]RedBack>clear circuit 3/0 all
```

The following example clears a range of ATM circuits, VPI:VCI `10:10` through `10:40`:

```
[local]RedBack>clear circuit 5/0 10 10 through 40
```

Related Commands

clear subscriber
show atm pvc
show frame-relay pvc
show subscribers

clear port counters

clear port counters *slot/port* [**hdlc-channel** *chan-name*] [**pvc** {**all** | *vpi* [*vci* [**through** *end-vci*]] | *dlci* [**through** *end-dlci*]} [**dot1q-pvc** {**all** | *vlan-id* | **untagged**}]] [**-noconfirm**]

Purpose

Clears the counters associated with the specified port, the specified permanent virtual circuits (PVCs) within a port, or the specified channels within a port.

Command Mode

administrator exec

Syntax Description

slot/port	Physical backplane slot number and the specific port number on a particular module.
hdlc-channel *chan-name*	Optional. Name of a High-level Data Link Control (HDLC) channel for which counters are to be cleared. This option is only available for channelized DS-3 ports.
pvc	Optional. Clears counters associated with all PVCs, a specific PVC, PVCs associated with a specific virtual path identifier (VPI), or a range of PVCs. This keyword is valid only for Asynchronous Transfer Mode (ATM) and Frame Relay ports.
all	Clears counters associated with all PVCs on the port.
vpi	Optional. Virtual path identifier (VPI) for an ATM circuit. This option is valid only for ATM ports. The range of values is 0 to 255.
vci	Optional. Virtual channel identifier (VCI) for an ATM circuit, or the beginning of a range of VCIs. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI in a range of PVCs for which counters are cleared.
dlci	Optional. Data-link connection identifier (DLCI) of a configured Frame Relay PVC. This option is valid only for Frame Relay ports.
through *end-dlci*	Optional. Last DLCI in a range of PVCs for which counters are cleared.
dot1q-pvc	Optional. Clears counters for 802.1Q PVCs defined on the ports or circuits.
all	Clears counters for all 802.1Q PVCs defined on the ports or circuits.
vlan-id	Virtual LAN (VLAN) ID for the 802.1Q PVC for which counters are cleared.

untagged	Clears untagged traffic counters on the ports or circuits.
-noconfirm	Optional. Specifies that the command is executed without prompting for a confirmation.

Default

All counters associated with the specified port are cleared.

Usage Guidelines

Use the **clear port counters** command to clear the counters associated with the specified port, the specified PVCs within a port, or the specified channels within a port. This command only affects the statistics available to the command line; corresponding Simple Network Management Protocol (SNMP) counters are not cleared.

Examples

The following example clears the counters for the ATM port `4/1`:

```
[local]RedBack#clear counters atm 4/1 -noconfirm
```

The following example clears the counters on the same port for PVCs in the range from `18:100` to `18:200`:

```
[local]RedBack#clear counters atm 4/1 pvc 18 100 through 200 -noconfirm
```

The following example clears the counters for ATM port `5/0`, VPI:VCI `1:1`, without the **-noconfirm** option:

```
[local]RedBack#clear counters atm 5/0 pvc 1 1

clear pvc counters for atm port 5/0 vpi 1 vci 1 [confirm] y
```

Related Commands

show port counters

clear port dot1q

clear port dot1q [*slot/port*]

Purpose

Clears the 802.1Q statistics for the specified port.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number for a particular port.

Default

Clears the 802.1Q statistics for all ports.

Usage Guidelines

Use the **clear port dot1q** command to clear the 802.1Q statistics for the specified port, or for all ports. This command only affects the statistics available to the command line; corresponding Simple Network Management Protocol (SNMP) counters are not cleared.

Examples

The following command clears the 802.1Q statistics for port 4 in slot 3:

```
[local]RedBack>clear port dot1q 3/4
```

Related Commands

bind dot1q
show port dot1q

debug hdlc

debug hdlc [*slot/port*]

no debug hdlc [*slot/port*]

Purpose

Enables the logging of Cisco High-level Data Link Control (HDLC) debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

slot/port	Optional. Backplane slot number and port number of a particular port. If you omit this argument, Cisco HDLC debugging is enabled for all ports configured with Cisco HDLC encapsulation.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug hdlc** command to enable the logging of HDLC debugging messages. This command is valid only for ports configured with Cisco HDLC encapsulation. When you enable HDLC debugging, Cisco HDLC-related messages are logged. Use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables HDLC debugging on a HDLC channels:

```
[local]RedBack#debug hdlc
```

Related Commands

logging console
show debugging
terminal monitor

description

description *text*

no description

Purpose

Assigns a textual description to a port, circuit, or channel.

Command Mode

circuit configuration
HDLC channel configuration
port configuration

Syntax Description

text	Text string that identifies the port. Can be any alphanumeric string, including spaces, that is not longer than one line.

Default

No description is associated with a port, circuit, or channel.

Usage Guidelines

Use the **description** command to associate additional information with the name of the port, circuit, or channel. This text is displayed by the **show port info** command.

Use the **no** form of this command to delete a previously created description. To change a description, simply create a new one and it overwrites the existing one.

Examples

The following example creates a description to note the location of ATM port `4/1`:

```
[local]RedBack(config)#port atm 4/1
[local]RedBack(config-port)#description to DSLAM in Rack 5, Shelf 4
```

Related Commands

show port info

ip host

ip host *ip-address mac-address*

no ip host *ip-address mac-address*

Purpose

Creates a static host entry in the system host table.

Command Mode

circuit configuration

Syntax Description

ip-address	IP address of the host.
mac-address	Media Access Control (MAC) address of the host.

Default

None

Usage Guidelines

Use the **ip host** command to install a permanent entry in the host table for a host where dynamic address resolution (using the Address Resolution Protocol [ARP]) is either not possible or not desired. You can also use it to statically indicate the outgoing interface to use to reach a particular host.

You must bind a circuit to an interface using the **bind interface** command before you can use this command. This command is not available on Point-to-Point Protocol (PPP)-encapsulated circuits.

Use the **no** form of this command to remove the specified entry from the host table.

Examples

The following example configures a host entry for a host with IP address `10.1.1.1` and MAC address `d3:9f:23:46:77:13` on an Asynchronous Transfer Mode (ATM) virtual circuit:

```
[local]RedBack(config)#port atm 3/1
[local]RedBack(config-port)#atm pvc 255 2047 profile ubr_pro encapsulation bridge1483
[local]RedBack(config-pvc)#bind interface atm_3_1 local
[local]RedBack(config-pvc)#ip host 10.1.1.1 d3:9f:23:46:77:13
```

Related Commands

bind interface
show ip host

mac address

mac address *mac-address*

no mac address

Purpose

Establishes the source Ethernet Media Access Control (MAC) address for Point-to-Point Protocol over Ethernet (PPPoE) packets sent on a circuit.

Command Mode

circuit configuration

Syntax Description

mac-address	48-bit Ethernet MAC address in the form *hh:hh:hh:hh:hh:hh*.

Default

None

Usage Guidelines

Use the **mac address** command to establish the source Ethernet MAC address for PPPoE packets sent for a circuit. This command can be entered for any circuit, as long as the circuit has the encapsulation set to PPPoE; this command does not apply to Ethernet ports. Once a source address has been set using this command, all PPPoE packets sent for this circuit use that MAC address as the source address.

Use the **no** form of this command to remove a previously established source MAC address.

Examples

The following example configures a MAC address for all PPPoE packets sent on an Asynchronous Transfer Mode (ATM) port:

```
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#atm pvc 155 566 profile atm4 encapsulation ppp
over-ethernet
[local]RedBack(config-pvc)#mac address 01:00:5e:00:00:00
```

Related Commands

atm pvc
frame-relay pvc

police

police rate *rate* **burst** *size*

{**no** | **default**} **police**

Purpose

Specifies a limit for the rate and burst tolerance of traffic received on a port.

Command Mode

port configuration

Syntax Description

rate *rate*	Rate in kbps. The range of values is 10 to 155520.
burst *size*	Burst tolerance in bytes. The range of values is 0 to 100000.

Default

Policing is disabled.

Usage Guidelines

Use the **police** command to limit the aggregate packet stream received from a port to the specified rate (in kilobits per second) and burst tolerance (in bytes). A reasonable rule of thumb for burst tolerance is 10 times the link maximum transmission unit (MTU), or around 15,000 to 20,000 bytes for subscriber circuits. A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and tolerance are dropped.

Use the **no** or **default** form of this command to disable any policing of traffic on the port.

Examples

The following example limits the rate and burst tolerance of incoming traffic by setting the rate to 200 kbps and the burst tolerance to `15,000` bytes:

```
[local]RedBack(config-port)#police rate 200 burst 15000
```

Related Commands

police—subscriber configuration mode
rate-limit

rate-limit

rate-limit rate *rate* **burst** *size*

{**no** | **default**} **rate-limit**

Purpose

Limits the aggregate packet stream transmitted on a port to the specified rate and burst tolerance.

Command Mode

port configuration

Syntax Description

rate *rate*	Rate in kbps. The range of values is 0 to 155,520.
burst *size*	Burst tolerance in bytes. The range of values is 0 to 100,000.

Default

Rate-limiting is disabled.

Usage Guidelines

Use the **rate-limit** command to limit the aggregate packet stream transmitted down a port to the specified rate and burst tolerance. A reasonable rule of thumb for burst tolerance is 10 times the link maximum transmission unit (MTU), or around 15,000 to 20,000 bytes for subscriber circuits. A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and tolerance are dropped.

Use the **no** or **default** form of this command to disable rate-limiting on the traffic transmitted from the port.

Examples

The following example places limits on the outgoing traffic from the port:

```
[local]RedBack(config-port)#rate-limit rate 100000 burst 15000
```

Related Commands

police
rate-limit—subscriber configuration mode

show port counters

show port counters [*slot/port*]

Purpose

Displays the counters associated with system ports.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a particular port for which counters are displayed.

Default

Displays summary information about all ports.

Usage Guidelines

Use the **show port counters** command to display counters associated with system ports. If the optional *slot/port* argument is provided, the output displays detailed counter information for the specified port; otherwise the output displays only summary counter information for all ports.

Table 9-3 describes the general port counters that are displayed for all port types. The “Examples” section contains information on other counters.

Table 9-3 show port counters: General Counters

Field	Description
pkts sent	Number of packets sent on the port
pkts rcvd	Number of packets received on the port
bytes sent	Number of bytes sent on the port
bytes rcvd	Number of bytes received on the port
mcast pkts sent	Number of multicast packets sent on the port
mcast pkts rcvd	Number of multicast packets received on the port
mcast bytes sent	Number of multicast bytes sent on the port
mcast bytes rcvd	Number of multicast bytes received on the port
xmt pkts dropped	Number of packets dropped during transmission

Table 9-3 show port counters: General Counters

Field	Description
rcv pkts dropped	Number of packets dropped during reception
xmt pkts outstanding	Number of packets left in the transmit queue
I/O buffers in rcv ring	Number of I/O buffers available in the receive ring
pkt xmt rate	Packet transmit rate (packets per second)
pkt rcv rate	Packet receive rate (packets per second)
port police drops	Number of packets dropped due to policing nonconformance on the port
port rate limit drops	Number of packets dropped due to rate-limiting nonconformance on the port
cct rate limit drops	Number of packets dropped due to circuit rate-limiting nonconformance (cumulative for all circuits on the port)
cct police drops	Number of packets dropped due to circuit-policing nonconformance (cumulative for all circuits on the port)
memory used	Amount of FE module memory (in bytes) that the port driver has consumed

Examples

The following example displays the counters for Ethernet port 0 in slot 2:

```
[local]RedBack>show port counters 2/0

TUE AUG 10 20:49:55 1999
General Counters:                   Last time cleared - never
    pkts sent = 0                          pkts rcvd = 0
    bytes sent = 0                         bytes rcvd = 0
    mcast pkts sent = 0                    mcast pkts rcvd = 0
    mcast bytes sent = 0                   mcast bytes rcvd = 0
    xmt pkts dropped = 0                   rcv pkts dropped = 0
    xmt pkts outstanding = 0               I/O buffers in rcv ring = 200
    pkt xmt rate = 0                       pkt rcv rate = 0
    port rate limit drops = 0              port police drops = 0
    cct rate limit drops = 0               cct police drops = 0
    memory used = 64724

Transmit Counters:
    jabber = 0                             underflow = 0
    lost carrier = 0                       no carrier = 0
    late collision = 0                     excessive collision = 0
    link failure = 0                       deferred = 0
    ok w/ collision = 0                    reclaimed = 0

Receive Counters:
    descrip errors = 0                     oversized frames = 0
    collisions = 0                         watchdog = 0
    mii errors = 0                         crc errors = 0
```

```
    dribble = 0                          overflow = 0
    runt frames = 0

Fatal Counters:
    bus parity errors = 0            bus master aborts = 0
    bus target aborts = 0            bus unknown errors = 0
```

The following example shows a detailed display for clear-channel DS-3 port 0 in slot 6:

```
[local]RedBack>show port counters 6/0

MON JUL 26 19:06:51 1999
General Counters:             Last time cleared - never
    pkts sent = 1660                 pkts rcvd = 1715
     bytes sent = 28418              bytes rcvd = 30178
    mcast pkts sent = 0              mcast pkts rcvd = 238
    mcast bytes sent = 0             mcast bytes rcvd = 6664
    xmt pkts dropped = 0             rcv pkts dropped = 0
    xmt pkts outstanding = 0         I/O buffers in rcv ring = 200
    pkt xmt rate = 0                 pkt rcv rate = 0
    port rate limit drops = 0        port police drops = 0
    cct rate limit drops = 0         cct police drops = 0
    memory used = 480
    tx_underflow = 0                 rx_bad_status = 0
    frame_too_big = 0                rx_abort = 0
    on-demand attempts = 0           on-demand errs = 0

    Local_Alarms  = 1                Remote_Alarms = 1
    Loss_of_Signal= 0                Out_of_Frame  = 1
    Alarm_Ind_Sig = 0
    Line Code Violations = 10        Frame Errors = 105
    Parity Errors = 2                Path Parity Errors  = 0
    FEBE Events = 0                  Line Status = no errors
```

Table 9-4 describes the counters in the display:

Table 9-4 show port counters: Clear-Channel DS-3 Counters

Field	Description
tx_underflow	Number of transmit underflow errors detected
rx_bad_status	Number of receive frames with bad status detected
frame_too_big	Number of frames exceeding the maximum length detected
rx_abort	Number of frames.
on-demand attempts	Number of on-demand circuit creation attempts from the driver
on-demand errs	Number of failed on-demand attempts to create a circuit
Local_Alarms	Number of local alarms detected
Remote_Alarms	Number of remote alarms detected
Loss_of_Signal	Number of times loss of signal was detected

Table 9-4 show port counters: Clear-Channel DS-3 Counters

Field	Description
Out_of_Frame	Number of out-of-frame errors.
Alarm_Ind_Sig	Number of alarm indication signals detected
Line Code Violations	Number of line code violations detected
Frame Errors	Number of frame errors detected
Parity Errors	Number of parity errors detected
Path Parity Errors	Number of M-frames in which the calculated parity of the received data bits of the previous M-frame does not match a majority vote of the three received CP bits (C-bits in subframe 30)
FEBE Events	Number of M-frames where any C-bit in subframe 4 is zero
Line status	OOF—Out of frame LOS—Loss of signal detected AIS—Alarm Indication Signal detected YELLOW—Yellow Alarm detected no errors—none of the above errors detected

The following example displays the counters for an ATM OC-3 port:

```
[local]RedBack>show port counters 6/0

WED SEP 01 15:23:44 1999>
General Counters:                Last time cleared - never
  pkts sent = 680273               pkts rcvd = 660706
  bytes sent = 310570009           bytes rcvd = 59441896
  xmt pkts dropped = 0             rcv pkts dropped = 0
  xmt pkts outstanding = 0         I/O buffers in rcv ring = 512
  pkt xmt rate = 22                pkt rcv rate = 25
  port rate limit drops = 0        port police drops = 0
  cct rate limit drops = 0         cct police drops = 0
  memory used = 274384

ATM Layer Counters (some delayed < 30 sec):
  cells sent = 6796807             cells rcvd = 1564798
  rcvd cells dropped = 11361       length_errs = 0
  pad errs = 4                     non-zero cpis = 1
  crc errs = 6                     timeout errs = 0
  pci bus errs = 0                 dma afull errs = 0
  fr parity errs = 0               fr sync errs = 0

Additional ATM Layer Counters:
  seg statusq ovfl errs = 0        seg null sbd info errs = 0
  seg get sbd info errs = 0        seg undf errs = 0
  seg host status full = 0
  rsm statusq ovfl errs = 0        rsm ba errs = 0
  rsm len errs = 0                 rsm ffpd errs = 0
  rsm epd errs = 0                 rsm undf errs = 0
  rsm ovfl errs = 0                rsm sfpd errs = 0
```

```
  rsm abort errs = 0
  on-demand attempts = 0          on-demand errs = 0

ATM Layer OAM Cell Counters (some delayed < 30 sec):
  total sent = 0                  total rcvd = 0
  f4 segment rcvd = 0             f4 end-to-end rcvd = 0
  f5 segment rcvd = 0             f5 end-to-end rcvd = 0
  pti 6 rcvd = 0                  pti 7 rcvd = 0
  loopback sent = 0               loopback rcvd = 0
  loopback resp sent = 0          loopback resp rcvd = 0
  ais sent = 0                    ais rcvd = 0
  rdi sent = 0                    rdi rcvd = 0

Physical Layer Error Counters (all delayed < 30 sec):
  line febe = 0       line ferf = 0       line ais = 0
  path febe = 0       path ferf = 0       path ais = 0
  path yellow = 1     sts lof23 = 1       sts lof = 1
  sts oof = 0         sts lop = 1         bip = 0
  loc = 0             los = 0             1 sec cnt = 1
  signal label mismatches = 0
```

Table 9-5 and Table 9-6 describe the ATM Layer Counters displayed in the output.

Table 9-5 show port counters: ATM Layer Counters

Field	Description
cells sent	Number of cells sent on the port
cells rcvd	Number of cells received on the port
rcvd cells dropped	Number of cells dropped during reception
length errs	AAL5 CPCS-PDU length exceeds the maximum length
pad errs	Length of the AAL5 pad field is incorrect
non-zero cpis	AAL5 CPI field is nonzero
crc errs	AAL5 CRC error or OAM CRC error
timeout errs	Number of times an AAL5 reassembly timeout error occurred
pci bus errs	Number of PCI bus errors
dma afull errs	Number of times a “DMA almost full” error condition occurred
fr parity errs	Number of frame parity errors on frames sent between the PHY and SAR
fr sync errs	Number of frame sync errors on frames sent between the PHY and SAR

Table 9-6 show port counters: Additional ATM Layer Counters

Field	Description
seg statusq ovfl errs	Number of overflow conditions for the segmentation status queue
seg null sbd info errs	Number of NULL SBD info pointers that were received
seg get sbd info errs	Number of failures to get SBD info pointers
seg undf errs	Number of underflow conditions for the segmentation status queue
seg host status full	Number of times the segmentation status queue was full
rsm statusq ovfl errs	Number of times that the reassembly status queue has overflowed
rsm ba errs	Number of times the total length of a reassembled PDU has exceeded the maximum defined length.
rsm len errs	Number of times the total length of a reassembled PDU has exceeded the maximum defined length
rsm ffpd errs	Number of DMA FIFO full-packet discard errors
rsm epd errs	Number of early packet discards
rsm undf errs	Number of free buffer queue underflows
rsm ovfl errs	Last available reassembly status queue entry
rsm sfpd errs	Number of status full packet discards
rsm abort errs	Number of times an abort function was detected
on-demand attempts	Number of attempted on-demand circuit creations
on-demand errs	Number of on-demand circuit creation failures

Table 9-7 shows the ATM layer Operations and Maintenance (OAM) cell counters.

Table 9-7 show port counters: ATM Layer OAM Cell Counters

Field	Description
total sent	Total number of OAM cells sent
total rcvd	Total number of OAM cells received
f4 segment rcvd	Number of F4 segment-to-segment cells received
f4 end-to-end rcvd	Number of F4 end-to-end cells received
F5 segment rcvd	Number of F5 segment-to-segment cells received
F5 end-to-end rcvd	Number of F5 end-to-end cells received
pti 6 rcvd	Number of cells with payload type identifier (PTI) value of six received
pti 7 rcvd	Number of cells with PTI value of seven received
loopback sent	Number of loopback cells sent
loopback rcvd	Number of loopback cells received

Table 9-7 show port counters: ATM Layer OAM Cell Counters

Field	Description
loopback resp sent	Number of loopback responses sent
loopback resp rcvd	Number of loopback responses received
ais sent	Number of OAM AIS cells sent
ais rcvd	Number of OAM AIS cells received
rdi sent	Number of OAM RDI cells sent
rdi rcvd	Number of OAM RDI cells received

Table 9-8 shows the physical layer error counters for ATM OC-3 ports, as shown in the example output.

Table 9-8 show port counters: Physical Layer Error Counters (for ATM OC-3 ports)

Field	Description
line febe	Set if any valid nonzero FEBE value is detected in the Z2 octet of the STS-1/STS-3c/STM-1 overhead
line ferf	Set if the three least significant bits of the K2 octet are set to '110' for five consecutive frames
line ais	Set if the three least significant bits of the K2 octet are set to '111' for five consecutive frames
path febe	Set if any valid nonzero FEBE value (1-8) is detected in the most significant nibble of the G1 octet of the STS-1/STS-3c/STM-1 overhead
path ferf	Set if a value of 9 is detected in the most significant nibble of the G1 octet of the STS-1/STS-3c/STM-1 overhead
path ais	Set if H1 and H2 octets are all ones for three consecutive frames
path yellow	Set if the path yellow bit in the G1 octet is set for 10 consecutive frames
sts lof23	Set if STS LOF is high for three consecutive one-second latching signals
sts lof	Set when STS OOF is active for 24 consecutive SONET frames
sts oof	Set if four consecutive A1/A2 framing patterns with errors are observed. For STS-3c/STM-1, the pattern observed consists of the third A1 octet and the first A2 octet
sts lop	Set if a valid pointer as defined in TR-NWT-000253 cannot be found in the H1/H2 pointer of the STS-1/STS-3c/STM-1 overhead
bip	Set if there is an error in any oof the B1, B2, or B3 BIP-8, or BIP-24 codes at the receiver (summary BIP error)
b1bip8	Number of section BIP errors
b2bip8_24	Number of line BIP errors
b3bip8	Number of STS path BIP errors
loc	Indicates that cell delineation has been lost (seven consecutive HEC errors occur at the current cell delineation position)
los	Set if loss of signal is detected

Table 9-8 show port counters: Physical Layer Error Counters (for ATM OC-3 ports)

Field	Description
plm	Number of path label mismatches
Section Status	Section alarms
Line Status	Line alarms
Path Status	Path alarms

Table 9-9 shows the physical layer error counters for ATM DS-3 ports (not included in the example output).

Table 9-9 show port counters: Physical Layer Error Counters (For ATM DS-3 ports)

Field	Description
plcp febe	Set if any valid nonzero FEBE value (1-8) is detected in the G1 octet in 57-octet PLCP formats
plcp bip	Set if there is an error in the BIP-8 code (B1 octet) checking in LCP formats
plcp frame	Set if there is an error in either the A1 or A2 octets of the PLCP frame pattern for 57-octet PLCP formats
plcp lof	Set when PLCP OOF is active for eight consecutive PLCP frames
plcp lof23	Set if PLCP LOF is high for three consecutive one-second latching signals
plcp yellow	(Path Yellow/LOC (loss of cell delineation)) Cell delineation is lost if seven consecutive HEC errors occur at the current cell delineation position. This bit is active for 53-octet formats using external framers or the parallel interface. For DS-3 module with direct-mapped cells, the PLCP indications should be ignored; only the LC and DS3 framer indications are meaningful
ds3 oof	Indicates tat the internal DS3 framer has lost frame alignment. An Out of Frame (OOF) condition for DS3 occurs when 3 out of 16 F-bits are in error, or 2 out of 3 M-frames contain M-bit errors
ds3 ais	Indicates that the internal DS3 framer has detected an Alarm Indication Signal (AIS). A DS3 AIS is a 1010... payload with valid framing and parity, equal X-0bits, and all C-bits set to zero
ds3 idle codes	Indicates that the internal DS3 framer has detected and idle code signal. A DS3 idle code is a 1100... payload with valid framing and parity, equal X-bits, and all subviral 3 C-bits set to zero
ds3 xbit yellow	Set if the internal DS3 framer detects both X1 and X3 low in an M-frame
los	Set if there is a loss of signal detected

Related Commands

show port info

show port diag

show port diag *slot/port*

Purpose

Displays hardware information for a port.

Command Mode

operator exec

Syntax Description

slot/port	Backplane slot number and port number for which information is displayed.

Default

None

Usage Guidelines

Use the **show port diag** command to display hardware information for a particular port. If the port is not present in the system, the display is empty.

Examples

The following example shows the backplane information for the console port (slot `0`, port `0`):

```
[local]pm1>show port diag 0/0

Slot/Port number 0/0
        STATE_PRESENT
        Description "DEC 21140"
        Vendor ID = 0x1011
        Device ID = 0x0009
        Sub Vendor ID = 0x11af
        Sub System ID = 0xf0ce
        Class = 02 Network Controller
        Sub Class = 0x00 Ethernet
        Base 1 = 0x50000000     size = 0x00000080
        Interrupt line = 0x0a
```

Related Commands

show port info
show diag

show port dot1q

show port dot1q [*slot/port*]

Purpose

Displays 802.1Q statistics for the specified port.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number for a particular port.

Default

802.1Q counters for all ports configured with an 802.1Q binding are displayed.

Usage Guidelines

Use the show port dot1q command to display 802.1Q counters for ports configured with the **bind dot1q** command.

Examples

The following command shows the 802.1Q statistics for all ports on the system configured with an 802.1Q binding:

```
[local]RedBack>show port dot1q

THU JAN 06 21:05:40 2000
    No. of                Packets                   Bad VIDs      Not
Port VIDs         Received       Transmitted      0     1  4095  Bound
---- ----    --------------      ------------  ----  ----  ----  -----
0/0    1             2000              2000     0     1     0      0
2/0    1             3000              3000     2     0     0      1
```

Table 9-10 describes the fields displayed in the **show port dot1q** command output:

Table 9-10 show port dot1q display fields

Field	Description
Port	System port number
VID	VLAN tag ID on the port.
Packets Received	Number of 802.1Q packets received on the port
Packets Transmitted	Number of 802.1Q packets sent on the port
Bad VIDs: 0	Number of packets received with an invalid VLAN ID value of 0
Bad VIDs: 1	Number of packets received with an invalid VLAN ID value of 1
Bad VIDs: 4095	Number of packets received with an invalid VLAN ID value of 4095
Not Bound	Number of packets received with a valid VLAN ID value other than that which to which the port was bound

Related Commands

bind dot1q
clear port dot1q
show port counters

show port info

show port info [*slot/port*]

Purpose

Displays the Media Access Control (MAC) address and other lower-layer settings of a single port or of all ports in the system.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a port for which information is displayed.

Default

Displays information for all ports in the system.

Usage Guidelines

Use the **show port info** command to display the MAC address and other lower-layer settings for a single port or for all ports in the system. If you include the *slot/port* argument, the output displays only information for the specified port. If the *slot/port* argument is not specified, the output includes all ports present in the system.

The information displayed varies depending on the type of port.

Examples

The following examples provide sample output of the **show port info** command for several different types of ports:

```
[local]RedBack>show port info 2/0

Port 2/0,  state is SHUTDOWN, driver type is ENET
MAC Address                 = 00:10:67:00:20:aa
Rate limit rate             = Disabled
Rate limit burst            = Disabled
Police rate                 = Disabled
Police burst                = Disabled
Loopback                    = Disabled
```

```
Binding                     = (none)
Port Speed                  = 10 Megabits
Line Mode                   = Half Duplex
[local]RedBack>show port info 3/0

Port 3/0,  state is SHUTDOWN, driver type is ATM
MAC Address                 = 00:10:67:00:22:bd
Rate limit rate             = Disabled
Rate limit burst            = Disabled
Police rate                 = Disabled
Police burst                = Disabled
Physical layer interface    = DS3
Loopback                    = none
Cell-delineation            = hcs
Payload scrambling          = enabled
Clock-source                = internal
Idle cell header            = 0x00000000
Idle cell data              = 0x5a
Cable length                = short ( <= 225 ft )
External 8KHz Timing        = disabled
Transmit Buffers            = 256
Receive Buffers             = 64

[local]RedBack>show port info 7/1

Port 7/1,  state is SHUTDOWN/UNCONFIGURED, driver type is FRAME
MAC Address                 = 00:10:67:00:60:da
Rate limit rate             = Disabled
Rate limit burst            = Disabled
Police rate                 = Disabled
Police burst                = Disabled
Physical layer interface    = T1
Port Speed                  = 1.544 Megabits
Loopback                    = none
Clock source                = internal
Cable length                = short
Framing                     = esf
Inverted data               = no
Transmit Buffers            = 200
Receive Buffers             = 200
```

Related Commands

show port counters
show port table

show port table

show port table

Purpose

Displays the ports that are present in the system, their current state, the driver type, and the port type.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show port table** command to display the ports that are present in the system, their current state, the driver type, and the port type.

Table 9-11 describes the values for the State field that can be displayed for a given port:

Table 9-11 Port Command States

State	Description
UP	Port is configured to be up, and it is up
DOWN	Port is configured to be up, and it is down
SHUTDOWN	Port is configured to be down, and it is down
SHUTDOWN/UNCONFIGURED	Port is not configured
EJECTOR_OPEN	Port ejectors are open.
EXTRACT_READY	Port is prepared for module hot-swap
UP/LOOPBACK	Port is configured for loopback and the link is up
DOWN/LOOPBACK	Port is configured for loopback and the link is down

Examples

The following example shows output from the **show port table** command:

```
[local]RedBack>show port table

I/O Port Table contents are:

Slot 0 port 0 state is UP driver type is ENET port type is 100BT.
Slot 2 port 0 state is UP driver type is ATM port type is OC3.
Slot 2 port 1 state is SHUTDOWN driver type is ATM port type is OC3.
```

Related Commands

show port counters
show port info

shutdown

shutdown

no shutdown

Purpose

Disables a port or High-level Data Link Control (HDLC) channel.

Command Mode

HDLC channel configuration
port configuration

Syntax Description

This command has no keywords or arguments.

Default

All ports and channels are shut down.

Usage Guidelines

Use the **shutdown** command to disable all functions on the port or HDLC channel. No data is transmitted or received when the port or channel is shut down. To check the port state, use the **show port table** operator exec command.

Use the **no** form of this command to enable a port.

Examples

The following example disables the ATM port `4/0`:

```
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#shutdown
```

The following example enables channel `c4` on port `6/0`:

```
[local]RedBack(config)#port channelized ds-3 6/0
[local]RedBack(config-port)#hdlc-channel c4
[local]RedBack(config-chan)#no shutdown
```

Related Commands

show port table

Ethernet Port Commands

This chapter describes the commands used to configure Ethernet ports under the Access Operating System (AOS). See also Chapter 9, “Common Port, Circuit, and Channel Commands” for descriptions for commands that apply across all port types.

For overview information, a description of the tasks used to configure Ethernet ports, and configuration examples, see “Configuring Ethernet Ports” in the *Access Operating System (AOS) Configuration Guide*. For information on how to configure the Ethernet management port, see the “Configuring the Management Port” section of the “Accessing the AOS and Configuring Terminal Settings” chapter in the *Access Operating System (AOS) Configuration Guide*.

encapsulation

encapsulation {**dot1q** | **ppp over-ethernet** | **multi**}

default encapsulation

Purpose

Specifies the encapsulation to be used on an Ethernet port.

Command Mode

port configuration

Syntax Description

dot1q	Specifies that the encapsulation for the port is 802.1Q, and enters dot1q encapsulation configuration mode.
ppp over-ethernet	Specifies that the encapsulation to be used on this port is PPP over Ethernet (PPPoE).
multi	Specifies that this Ethernet port contains both IP over Ethernet and PPPoE.

Default

The default encapsulation is IP over Ethernet.

Usage Guidelines

Use the **encapsulation** command to set the encapsulation type on an Ethernet port to 802.1Q, PPPoE, or a combination of PPPoE and IP over Ethernet.

When you use the **dot1q** keyword to specify 802.1Q encapsulation, you can create 802.1Q permanent virtual circuits (PVCs). You cannot specify **dot1q** encapsulation on the Ethernet management port.

Use the **default** form of this command to reset the port to IP over Ethernet encapsulation.

Examples

The following example shows an Ethernet port being set to use PPPoE encapsulation:

```
[local]RedBack(config)#port ethernet 2/0
[local]RedBack(config-port)#encapsulation ppp over-ethernet
```

The following example shows an Ethernet port being set to use either PPPoE or IP over Ethernet encapsulation:

```
[local]RedBack(config)#port ethernet 2/1
[local]RedBack(config-port)#encapsulation multi
```

Related Commands

show configuration

ip host

ip host *ip-address mac-address*

no ip host *ip-address mac-address*

Purpose

Creates a static host entry in the system host table.

Command Mode

port configuration

Syntax Description

ip-address	IP address of the host.
mac-address	MAC address of the host.

Default

None

Usage Guidelines

Use the **ip host** command to install a permanent entry in the host table for a host where dynamic address resolution (ARP) is either not possible or not desired. You can also use it to statically indicate the outgoing interface to use to reach a particular host.

An Ethernet port must be bound to an interface (see the **bind interface** port configuration command) in order to use this command.

Use the **no** form of this command to remove the specified entry from the host table.

Examples

The following example configures a host entry for a host with IP address `10.1.1.1` and hardware address `d3:9f:23:46:77:13` on an Ethernet port:

```
[local]RedBack(config)#port ethernet 5/0
[local]RedBack(config-port)#bind interface ether_5_0 local
[local]RedBack(config-port)#ip host 10.1.1.1 d3:9f:23:46:77:13
```

Related Commands

bind interface
show configuration
show ip host

loopback

loopback

{**no** | **default**} **loopback**

Purpose

Creates a loopback on an Ethernet port.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to create a loopback on the Ethernet port. This command is typically used for testing purposes.

Use the **no** or **default** forms of this command to disable loopback on an Ethernet port.

Examples

The following example configures an Ethernet port to operate in loopback mode:

```
[local]RedBack(config)#port ethernet 6/0
[local]RedBack(config-port)#loopback
```

Related Commands

show port info

medium

medium {**auto** | **speed** {**10** | **100** | **1000**} **duplex** {**half** | **full**}}

{**no** | **default**} **medium**

Purpose

Sets the Ethernet port speed and duplex mode.

Command Mode

port configuration

Syntax Description

auto	Specifies that the port should auto-sense whether it is connected to a 10-Mbps or 100-Mbps Ethernet segment and the duplex mode of that segment.
speed {**10** | **100** | **1000**}	Sets the Ethernet port speed in Mbps.
duplex {**half** | **full**}	Sets the port duplex mode to either **half** (half-duplex) or **full** (full-duplex).

Default

Ethernet ports are set to auto-sense the speed and full duplex mode.

Usage Guidelines

Use the **medium** command to configure the port speed and duplex mode. Use the **speed** keyword to force an Ethernet port to use the specified speed and duplex mode.

Use the **no** or **default** form of this command to restore the settings to auto-sense both the speed and duplex mode.

Examples

The following example manually configures an Ethernet port to use a speed of 10 Mbps and full-duplex mode:

```
[local]RedBack(config)#port ethernet 4/1
[local]RedBack(config-port)#medium speed 10 duplex full
```

Related Commands

show port info

port ethernet

port ethernet *slot/port*

Purpose

Enters port configuration mode for the specified Ethernet port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port ethernet** command to enter port configuration mode to configure an Ethernet port on the system, including the Ethernet management port.

The management port is an Ethernet port on the system that is designated for system management. The location of this port varies, depending on the hardware platform:

- The management port on a Subscriber Management System (SMS) 500, SMS 1000, or SMS 1800 is located on the Control Engine (CE) module in slot 0. The management port is 0/0.
- The management port on an SMS 10000 is located on an Ethernet Management module that is associated with a System Management (SM) module. The SMS 10000 supports redundant SM modules (SM-2 and SM-3), and redundant Ethernet Management modules. The Ethernet Management module associated with SM-2 is in slot 4; the Ethernet Management module associated with SM-3 is in slot 6. In a redundant configuration, only one SM module and one Ethernet Management module is active at a time. The active management port on a system is port 0 on the active Ethernet Management module. Use the following guidelines when configuring the management port on an SMS 10000:
  - — The management port is 4/0 when SM-2 is active and 6/0 when SM-3 is active.
  - — The Access Operating System (AOS) accepts configuration commands for either port 4/0 or 6/0, regardless of which SM module is active. AOS always applies these commands to the active management port.

Note The configuration for 4/0 and 6/0 must be the same. If you edit a configuration file offline, be sure the configuration for these ports is the same. The port configuration commands for 4/0 and 6/0 are executed in order on the active management port, and if the configuration for these ports is not consistent, you may not achieve the desired configuration.

— The **show configuration** administrator exec command shows identical configuration information for port 4/0 and 6/0.

— The **save configuration** administrator exec command saves identical configuration information for port 4/0 and 6/0.

Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first Ethernet port on the module in slot 4 on an SMS 10000 and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port ethernet 4/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

radius attribute medium-type

radius attribute medium-type {**dsl** | **cable** | **wireless** | **satellite**}

{**no** | **default**} **radius attribute medium-type**

Purpose

Specifies the value that AOS supplies for the Medium-Type vendor-specific attribute (VSA) in Remote Access Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets.

Command Mode

port configuration

Syntax Description

dsl	Specifies that the value of the Medium-Type VSA is DSL.
cable	Specifies that the value of the Medium-Type VSA is cable.
wireless	Specifies that the value of the Medium-Type VSA is wireless.
satellite	Specifies that the value of the Medium-Type VSA is satellite.

Default

The Medium-Type attribute is not sent.

Usage Guidelines

For Ethernet ports, this command specifies the value of the Medium-Type attribute for any PPP over Ethernet sessions that arrive at the SMS over the port.

The **no** and **default** forms of this command perform the same function which is to disable the sending of the attribute.

Note This command description is repeated in the “RADIUS Commands” chapter.

Examples

In the following example, the sessions that arrive over the specified Ethernet port are configured to be associated with cable subscribers:

```
[local]RedBack(config)#port ethernet 3/0
[local]RedBack(config-port)#radius attribute medium-type cable
[local]RedBack(config-port)#encapsulation ppp over-ethernet
```

```
[local]RedBack(config-port)#bind authentication chap pap
```

Related Commands

aaa accounting

ATM Port Commands

This chapter describes the commands use to configure all types of Asynchronous Transfer Mode (ATM) ports through the Access Operating System (AOS).

See Chapter 9, “Common Port, Circuit, and Channel Commands,” for descriptions for commands that apply to all port types.

For overview information, a description of the tasks used to configure ATM ports, and configuration examples, see the “Configuring ATM Ports” chapter in the *Access Operating System (AOS) Configuration Guide*.

8khztiming

8khztiming

{**no** | **default**} **8khztiming**

Purpose

Forces the transmit Physical Layer Convergence Protocol (PLCP) to use an external 8kHz timing reference, rather than the received PLCP reference, on Asynchronous Transfer Mode (ATM) DS-3 ports.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

The transmit PLCP synchronizes to the received PLCP reference.

Usage Guidelines

Use the **8khztiming** command to force the transmit PLCP to use an external 8kHz timing reference.

Note This command applies only to ATM DS-3 ports.

Use the **no or default form** of this command to disable external 8kHz reference timing.

Examples

The following example causes the upper ATM DS-3 port in slot 3 to use an external 8kHz timing reference:

```
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#8khztiming
```

Related Commands

atm profile
show port info

cablelength

cablelength {**long** {**0db** | **-7.5db** | **-15db** | **-22.5db**} | **short** {**110** | **220** | **330** | **440** | **550** | **660**}}

default cablelength

Purpose

Specifies the length of the attached T1 cable or the transmit output power.

Command Mode

port configuration

Syntax Description

long	Indicates a long cable (over 660 ft).
0db	Specifies a transmit power level of 0 decibels.
-7.5db	Specifies a transmit power level of –7.5 decibels.
-15db	Specifies a transmit power level of –15 decibels.
-22.5db	Specifies a transmit power level of –22.5 decibels.
short	Indicates a short cable (up to 660 ft).
110	Specifies a cable length of up to 110 ft.
220	Specifies a cable length of up to 220 ft.
330	Specifies a cable length of up to 330 ft.
440	Specifies a cable length of up to 440 ft.
550	Specifies a cable length of up to 550 ft.
660	Specifies a cable length of up to 660 ft.

Default

The default is **short**, up to **110** ft.

Usage Guidelines

Use the **cablelength** command to specify the length and transmit power level for the cable attached to an Asynchronous Transfer Mode (ATM) T1 port. When you use the **short** keyword, the length specified indicates that your cable is equal to or less than the value. For example, the **cablelength short 440** command indicates that the cable is between 331 and 440 ft. When you use the **long** keyword, you must also specify the transmit power level.

Use the **default** form of this command to return the settings to the default values.

Examples

The following example sets the cablelength to between 331 and 440 ft:

```
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#cablelength short 440
```

Related Commands

show port info

cell-delineation

cell-delineation {**hcs** | **plcp**}

default cell-delineation

Purpose

Changes the cell delineation used on an Asynchronous Transfer Mode (ATM) DS-3 or ATM E3 port.

Command Mode

port configuration

Syntax Description

hcs	Configures the port to use framing based on header check sequence (HCS) for cell delineation.
plcp	Configures the port to use framing based on Physical Layer Convergence Protocol (PLCP) for cell delineation.

Default

HCS framing is used for cell delineation.

Usage Guidelines

Use the **cell-delineation** command to modify the desired framing on an ATM DS-3 or ATM E3 port. This command only applies to ATM DS-3 ports.

Use the **default** form of this command to set the cell delineation to HCS.

Examples

The following example changes the cell delineation on an ATM DS-3 port in slot 4 to PLCP:

```
[local]RedBack(config)#port atm 4/1
[local]RedBack(config-port)#cell-delineation plcp
```

Related Commands

show port info

clock-source

clock-source {**internal** | **line**}

no clock-source

Purpose

Configures the source of the transmit data clock on an Asynchronous Transfer Mode (ATM) port.

Command Mode

port configuration

Syntax Description

internal	Specifies that the transmit clock is generated internally by the port.
line	Specifies that the transmit clock is derived from the received clock.

Default

The transmit clock is generated internally.

Usage Guidelines

Use the **clock-source** command to configure the source of the transmit data clock on an ATM port.

Use the **no** form of this command to configure the port to generate the transmit clock internally.

Examples

The following example changes port 1 in slot 4 to use a transmit clock derived from the received clock:

```
[local]RedBack(config)#port atm 4/1
[local]RedBack(config-port)#clock-source line
```

Related Commands

show port info

fdl

fdl {**ansi** | **att**}

no fdl

Purpose

Enables the transmission of performance reports for the T1 port using the Facility Data Link (FDL) per ANSI T1.403.

Command Mode

port configuration

Syntax Description

ansi	Enables a one-second transmission of the performance report.
att	Enables a 15-minute transmission of the performance report.

Default

Performance reports are disabled.

Usage Guidelines

Use the **fdl** command to enable the transmission of performance reports for the T1 port using the FDL.

Note This command is available only for Asynchronous Transfer Mode (ATM) T1 ports that are configured with Extended Superframe (ESF) framing.

Use the **no** form of this command to disable the transmissions.

Examples

The following example enables a one-second transmission of the performance report:

```
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#fdl ansi
```

Related Commands

framing
show port info

framing

framing {**esf** | **sf** | **crc4** | **no-crc4** | **stm1** | **stm4** | **g751** | **g832**}

default framing

Purpose

Configures the framing for an Asynchronous Transfer Mode (ATM) port.

Command Mode

port configuration

Syntax Description

esf	Specifies Extended Superframe Format (ESF). This option is available only for ATM T1 ports.
sf	Specifies Superframe Format (or D4). This option is available only for ATM T1 ports
crc4	Specifies CRC4 framing, per the ITU G.704 specification. This option is available only for ATM E1 ports.
no-crc4	Specifies no CRC4 framing per the ITU G.704 specification. This option is available only for ATM E1 ports.
stm1	Specifies SDH/STM-1 framing. This option is available only for ATM OC-3 ports.
stm4	Specifies SDH/STM-4 framing. This option is available only for ATM OC-12 ports.
g751	Specifies G.751Physical Layer Convergence Protocol (PLCP) framing. This option is available only for ATM E3 ports.
g832	Specifies G.832 framing. This option is available only for ATM E3 ports.

Default

For ATM OC-3 ports, the framing is SONET/STS-3c; for ATM OC-12 ports, the framing is SONET/STS-12c; for ATM T1 ports, the framing is ESF; for ATM E1 ports, the framing is CRC4; for ATM E3 ports, the framing is G.751.

Usage Guidelines

Use the **framing** command to configure the framing for an ATM port.

Note This command does not apply to ATM DS-3 ports.

The keywords available vary based upon the port type. For ATM OC-3 ports, the **stm1** keyword changes the framing from SONET/STS-3c to SDH/STM-1. For ATM OC-12 ports, the **stm4** keyword changes the framing from SONET/STS-12c to SDH/STM-4.

Use the **default** form of this command to set the framing back to the default value for the port type.

Examples

The following example sets the framing on an ATM T1 port to Superframe Format:

```
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#framing sf
```

Related Commands

show port info

idle-cell

idle-cell {**header** *header-value* | **payload** *payload-value*}

default idle-cell {**header** | **payload**}

Purpose

Changes the header or payload value of idle cells sent on an Asynchronous Transfer Mode (ATM) port.

Command Mode

port configuration

Syntax Description

header *header-value*	4-byte hexadecimal value to be sent in the header for idle cells. The value must be preceded by "0x" to indicate that a hexadecimal value. The default header value is 0x00000000.
payload *payload-value*	1-byte hexadecimal value to be sent in the payload for an idle cell. The value must be preceded by "0x" to indicate a hexadecimal value. The default payload value is 0x5A.

Default

Idle-cells use a header value of 0x00000000 and a payload value of 0x5A.

Usage Guidelines

Use the **idle-cell** command to configure the header or payload value of idle cells sent on an ATM port.

Note This command applies only to ATM DS-3 and OC-3 ports.

Note You can only configure nonzero values in bits 1 to 3 of octet 4 for the idle-cell header; otherwise, the cells are not recognized as idle cells.

Use the **default** form of this command to reset the idle cell header and payload to the default value.

Examples

The following example modifies the bit pattern used for idle cell headers and payloads on ATM port `4/1`:

```
[local]RedBack(config)#port atm 4/1
```

```
[local]RedBack(config-port)#idle-cell payload 0x55
[local]RedBack(config-port)#idle-cell header 0x0002
```

Related Commands

show port info

length

length {**short** | **long**}

default length

Purpose

Sets the line length of the physical cable that is attached to an Asynchronous Transfer Mode (ATM) DS-3 port.

Command Mode

port configuration

Syntax Description

short	Specifies the attached cable is less than or equal to 225 ft.
long	Specifies the attached cable is greater than 225 ft.

Default

The line length is less than or equal to 225 ft.

Usage Guidelines

Use the **length** command to specify the length of the cable attached to an ATM DS-3 port.

Note This command is available for ATM DS-3 ports only.

Use the **default** form of this command to configure the port to use a cable that is 225 ft or less in length (short).

Examples

The following example configures an ATM DS-3 port for use with a long cable:

```
[local]RedBack(config)#port atm 7/0
[local]RedBack(config-port)#length long
```

Related Commands

show port info

linecode

linecode {**ami** | **b8zs**}

default linecode

Purpose

Changes the line coding for an Asynchronous Transfer Mode (ATM) T1 port.

Command Mode

port configuration

Syntax Description

ami	Specifies alternate mark inversion (AMI) as the line coding.
b8zs	Specifies B8ZS as the line coding.

Default

The port uses B8ZS line coding.

Usage Guidelines

Use the **linecode** command to configure the line coding for an ATM T1 port.

Note This command applies only to ATM T1 ports.

Use the **default** form of this command to set the line coding to the default (B8ZS).

Examples

The following example sets the line coding to `AMI`:

```
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#linecode ami
```

Related Commands

show port info

loopback

loopback {**internal** | **line** | **local**}

{**no** | **default**} **loopback**

Purpose

Establishes a loopback on an Asynchronous Transfer Mode (ATM) port.

Command Mode

port configuration

Syntax Description

internal	Specifies loopback at the Segmentation and Reassembly (SAR) level (connects SAR transmit to SAR receive).
line	Specifies loopback at the physical layer (PHY) line level (connects PHY receive to PHY transmit).
local	Specifies loopback at the PHY source level (connects PHY transmit to PHY receive).

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to establish a loopback on an ATM port. This command is typically used for testing purposes. This command has identical syntax for both ATM OC-3 ports and ATM DS-3 ports.

Use the **no** or **default** form of this command to disable loopback.

Examples

The following example configures an ATM port to operate in loopback at the PHY source level:

```
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#loopback local
```

Related Commands

show port info

port atm

port atm *slot/port*

Purpose

Enters port configuration mode to configure an ATM port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port atm** command to enter port configuration mode to configure any type of ATM port on the system.

Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first ATM port on the module in slot 3 of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

scramble

scramble

no scramble

Purpose

Enables payload scrambling on an Asynchronous Transfer Mode (ATM) port.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

Payload scrambling is disabled.

Usage Guidelines

Use the **scrambling** command to enable payload scrambling on an ATM port.

Use the **no** form of this command to disable payload scrambling on the port.

Examples

The following example enables payload scrambling on port `atm 3/1`:

```
[local]RedBack(config)#port atm 3/1
[local]RedBack(config-port)#scramble
```

Related Commands

show port info

yellow-alarm

yellow-alarm {**detection** | **generation**}

no yellow-alarm {**detection** | **generation**}

default yellow-alarm {**detection** | **generation**}

Purpose

Enables detection or generation of a yellow alarm on an Asynchronous Transfer Mode (ATM) Tl or E1 port.

Command Mode

port configuration

Syntax Description

detection	Enables yellow alarm detection.
generation	Enables yellow alarm generation.

Default

Detection and generation of a yellow alarm are enabled.

Usage Guidelines

Use the **yellow-alarm** command to enable the detection or generation of yellow alarms. This command applies only to ATM T1 and ATM E1 ports.

Use the **no** form of this command to disable detection or generation of yellow alarms.

Use the **default** form of this command to enable both detection and generation of yellow alarms.

Examples

The following example enables both yellow alarm detection and generation:

```
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#yellow-alarm detection
[local]RedBack(config-port)#yellow-alarm generation
```

Related Commands

show port info

Channelized DS-3 Port Commands

This chapter describes the commands used to configure and maintain channelized DS-3 ports through the Access Operating System (AOS).

Chapter 9, “Common Port, Circuit, and Channel Commands,” describes commands that apply to all port types.

For overview information, a description of the tasks used to configure channelized DS-3 ports, and configuration examples, see the “Configuring Channelized DS-3 Ports” chapter in the *Access Operating System (AOS) Configuration Guide*.

bert

bert *slot/port* **t1** *t1-channel* **pattern** {**2^15** | **2^20** | **2^23** | **0s** | **1s**} **interval** *minutes*

no bert *slot/port* **t1** *t1-channel*

Purpose

Enables bit error rate testing (BERT) on the specified T1 channel on a channelized DS-3 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and the specific port number on a particular module.
t1 *t1-channel*	T1 channel on the channelized DS-3 port. The range of values is 1 to 28.
pattern	Specifies the test data pattern.
2^15	Specifies a 2^15 test pattern.
2^20	Specifies a 2^20 test pattern.
2^23	Specifies a 2^23 test pattern.
0s	Specifies all zeros as the test pattern.
1s	Specifies all ones as the test pattern.
interval *minutes*	Number of minutes to run testing.

Default

None

Usage Guidelines

Use the **bert** command to enable bit error rate testing on a T1 channel of a channelized DS-3 port.

Use the **no** form of this command to disable testing.

Examples

The following example enables BERT on port `5/1`, T1 channel `1`, using a test pattern of all zeros, for `10` minutes:

```
[local]RedBack#bert 5/1 t1 1 pattern 0s interval 10
```

Related Commands

clear bert
loopback
show bert

clear bert

clear bert *slot/port* **t1** {*t1-channel* | **all**}

Purpose

Clears bit error rate test (BERT) counters for a T1 channel on a channelized DS-3 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and port number of the port being tested.
t1	Indicates which T1 channel is cleared.
t1-channel	T1 channel on a channelized DS-3 port being tested.
all	Specifies that BERT counters on all T1 channels are cleared.

Default

None

Usage Guidelines

Use the **clear bert** command to clear bit error rate test (BERT) counters for a specific T1 channel or all T1 channels in a channelized DS-3 port.

Examples

The following shows output for slot 4, port 1, T1 channel 1:

```
[local]RedBack#clear bert 4/1 t1 1
```

Related Commands

bert
show bert

clear pmon

clear pmon *slot/port* {**all** | *t1-channel*} [**-noconfirm**]

Purpose

Clears all performance monitoring information for a T1 channel on a DS-3 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and port number of the configured port.
all	Specifies that all performance monitoring information for all T1 channels on the channelized DS-3 port is cleared.
t1-channel	T1 channel for which performance monitoring information is cleared.
-noconfirm	Optional. Specifies that no confirmation prompt appears before the command is run.

Default

None

Usage Guidelines

Use the **clear pmon** command to clear all performance monitoring information for all T1 channels or a specific T1 channel on a DS-3 port.

Examples

The following example clears the performance monitoring information for all T1 channels on a channelized DS-3 port:

```
[local]RedBack#clear pmon 5/0 all -noconfirm
```

Related Commands

show pmon

clock-source

clock-source {**internal** | **line**}

default clock-source

Purpose

Selects the source for the transmit clock for a DS-3 framer or a T1 channel.

Command Mode

port configuration
T1 channel configuration

Syntax Description

internal	Specifies the onboard clock as the source.
line	Specifies the derived receive clock as the source.

Default

The source for the transmit clock is the onboard clock (internal).

Usage Guidelines

Use the **clock-source** command to specify the source for the transmit clock for the DS-3 framer.

Use the **default** form of this command to set the clock source to internal.

Examples

The following example sets the transmit clock source to the derived receive clock:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#clock-source line
```

Related Commands

show port info

crc

crc {**16** | **32**}

default crc

Purpose

Sets the cyclic redundancy check (CRC) length.

Command Mode

HDLC channel configuration

Syntax Description

16	Specifies a 16-bit CRC.
32	Specifies a 32-bit CRC.

Default

The default CRC length is 16 bits.

Usage Guidelines

Use the **crc** command to set the length of the CRC for a High-level Data Link Control (HDLC) channel. The CRC determines if there have been any errors in data transmission, reading, or writing.

Use the **default** form of this command to set the CRC length to 16 bits.

Examples

The following example sets the CRC length to a 32 bits:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#hdlc-channel 1 t1 1
[local]RedBack(config-chan)#crc 32
```

Related Commands

hdlc-channel

encapsulation

encapsulation {**cisco-hdlc** | **frame-relay** | **ppp**}

default encapsulation

Purpose

Sets the encapsulation type for a High-level Data Link Control (HDLC) channel on a channelized DS-3 port.

Command Mode

HDLC channel configuration

Syntax Description

cisco-hdlc	Specifies the encapsulation type as Cisco HDLC (Cisco's proprietary HDLC encapsulation of IP) or other higher layer protocol.
frame-relay	Specifies the encapsulation type as Frame Relay.
ppp	Specifies the encapsulation type as RFC 1662, *PPP in HDLC-like Framing*.

Default

The default encapsulation type is Frame Relay.

Usage Guidelines

Use the **encapsulation** command to configure the encapsulation on an HDLC channel. The port and HDLC channel commands that are available depend upon the encapsulation type specified by this command. For example, if Cisco HDLC is specified, none of the Frame Relay commands (such as **frame-relay pvc** and **frame-rely intf-type**) apply.

Use the **default** form of this command to configure the channel to the default encapsulation, Frame Relay.

Examples

The following example specifies PPP encapsulation on an HDLC channel within a channelized DS-3 port and binds subscriber `george` in the local context:

```
[local]RedBack(config)#port channelized-ds3 4/1
[local]RedBack(config-port)#hdlc-channel george t1 1 timeslots 1-24
[local]RedBack(config-chan)#encapsulation ppp
[local]RedBack(config-chan)#bind subscriber george@local
```

Related Commands

bind authentication
bind interface
bind subscriber
keepalive

fdl

fdl {**ansi** | **att**}

no fdl

Purpose

Enables a one-second transmission of the performance report for the T1 channel using the Facility Data Link (FDL) per ANSI T1.403.

Command Mode

T1 channel configuration

Syntax Description

ansi	Enables one-second transmission of the performance report.
att	Enables the sending of a 15-minute transmission of the performance report.

Default

Performance reports are disabled by default.

Usage Guidelines

Use the **fdl** command to enable performance reporting for a T1 channel. This command is only available for T1 channels that are configured with Extended Superframe Format (ESF) framing.

Use the **no** form of this command to disable the transmissions.

Examples

The following example shows enabling a one-second transmission of the performance report:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#t1 3
[local]RedBack(config-t1)#fdl ansi
```

Related Commands

show t1 info

framing

framing {**c-bit** | **m23** | **esf** | **sf**}

default framing

Purpose

Selects the DS-3 framing.

Command Mode

port configuration
T1 channel configuration

Syntax Description

c-bit	Specifies C-bit framing. Available only for DS-3 ports.
m23	Specifies M23 framing. Available only for DS-3 ports.
esf	Specifies Extended Superframe Format (ESF) framing. Available only for T1 channels.
sf	Specifies Superframe Format (or D4) framing. Available only for T1 channels.

Default

The framing for channelized DS-3 ports is set to C-bit.

The framing for T1 channels in a DS-3 port is set to ESF.

Usage Guidelines

Use the **framing** command to configure the framing for a DS-3 port, or for a T1 channel within the DS-3 port.

Use the **default** form of this command to set the framing back to the default value.

Examples

The following command sets the framing for the channelized DS-3 port to `M23`, then sets the framing for T1 channel `1` to `SF`:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#framing m23
[local]RedBack(config-port)#t1 1
```

```
[local]RedBack(config-port)#framing sf
```

Related Commands

show port info
show t1 info

hdlc-channel

hdlc-channel *name* **t1** *t1-channel* **timeslot** *range*

no hdlc-channel *name*

Purpose

Creates or selects a High-level Data Link Control (HDLC) channel on a channelized DS-3 port and enters HDLC channel configuration mode.

Command Mode

port configuration

Syntax Description

name	Name of the HDLC channel.
t1 *t1-channel*	Constituent T1 channels that comprise the HDLC channel.
timeslot *range*	DS-0 channels within the T1 that comprise the HDLC channel. The range of values is 1 to 24. Commas and hyphens are allowed.

Default

No HDLC channels are defined.

Usage Guidelines

Use the **hdlc-channel** command to create and configure an HDLC channels within a channelized DS-3 port.

Use the **no** form of this command to delete the named HDLC channel.

Examples

The following example creates an HDLC channel called `c1:1-14` on the T1 channel `1`:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#hdlc-channel c1:1-14 t1 1 timeslot 1-14
```

Related Commands

show hdlc-config
show port info

invert-data

invert-data

{**no** | **default**} **invert-data**

Purpose

Inverts the polarity of all bits in the High-level Data Link Control (HDLC)-encoded stream.

Command Mode

HDLC channel configuration

Syntax Description

This command has no keywords or arguments.

Default

The default is no inversion.

Usage Guidelines

Use the **invert-data** command to invert the polarity of all bits in the HDLC-encoded stream.

Use the **no** or **default** form of this command to return the bits in the HDLC-encoded data stream to the original polarity.

Examples

The following example inverts the polarity on the HDLC-encoded data stream on an HDLC channel in a T1 port:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#hdlc-channel 1 t1 1
[local]RedBack(config-chan)#invert-data
```

Related Commands

hdlc-channel

keepalive

keepalive *seconds*

no keepalive

default keepalive

Purpose

Sets the period in seconds between keepalives sent on the High-level Data Link Control (HDLC) channel.

Command Mode

HDLC channel configuration

Syntax Description

seconds	Number of seconds between keepalives sent on the line. The default value is 10.

Default

The default number of seconds between keepalives is 10.

Usage Guidelines

Use the **keepalive** command to specify the number of seconds between keepalives sent on the HDLC channel. This command is only available in HDLC channel configuration mode when the encapsulation has been set to Cisco HDLC. The number of seconds must match the value configured on the interface of the router to which this line is connected.

Use the **no** form of the command to turn keepalives off so that connections are allowed to time out and terminate during periods of idleness.

Use the **default** form of the command to set the time between keepalives to the default value of 10 seconds.

Examples

The following example sets the time between keepalives to `20` seconds:

```
[local]RedBack(config-chan)#keepalive 20
```

Related Commands

encapsulation

length

length {**long** | **short**}

default length

Purpose

Specifies the length of the attached DS-3 (coaxial cable).

Command Mode

port configuration

Syntax Description

long	Specifies that the cable is longer than 225 feet.
short	Specifies that the cable is 225 feet or shorter.

Default

The cable length is set to 225 feet or shorter.

Usage Guidelines

Use the **length** command to configure the length of the cable attached to the DS-3 port.

Use the **default** form of this command to set the cable length to be 225 feet or shorter.

Examples

The following example sets the cable length to be longer than 225 feet:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#length long
```

Related Commands

show port info

loopback

loopback {**line** | **local** | **remote** [**ds3** | **t1** {**all** | *t1-channel*}]}

no loopback

Purpose

Creates a loopback on a channelized DS-3 port or one or more T1 channels on the port.

Command Mode

port configuration
T1 channel configuration

Syntax Description

line	Specifies that the receive line of the channelized DS-3 port (port configuration) or T1 channel (T1 channel configuration) is looped to the transmit line.
local	Specifies that all locally generated frames are looped back to the receiver for the channelized DS-3 port (port configuration) or a T1 channel (T1 channel configuration).
remote	Puts the far end in loopback for the channelized DS-3 port or for one or all T1 channels on the port, depending on the arguments specified. In port configuration mode, this command is only available if the port framing is set to C-bit. This option is only available in port configuration mode.
ds3	Places the far end of the DS-3 port in remote loopback. This option is available only in port configuration mode.
t1 {**all** | *t1-channel*}	Places the far end of the specified T1 channel, or all T1 channels on the DS-3 port in remote loopback.

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to establish a loopback on a channelized DS-3 port, or a T1 channel. Follow these guidelines:

- Use the **line** keyword to loop received data back to the transmit line for the channelized DS-3 port or T1 channel.

- Use the **local** keyword to loop locally generated frames back to the receiver for the channelized DS-3 port or T1 channel.
- Use the **remote ds3** keyword to verify remote link connectivity and quality at the DS-3 signal level.
- Use the **remote t1** keyword to perform remote link verification on a single DS-1 signal, or on all 28 individual DS-1 signals.

After creating a loopback, you can use the **bert** command to perform bit error rate testing to qualify the links.

Use the **no** form of this command to disable loopback.

Examples

The following command creates a line loopback on a channelized DS-3 port:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#loopback line
[local]RedBack(config-port)#end
[local]RedBack#bert t1 1 pattern 2^15 interval 5
```

Related Commands

bert
framing
show bert
show port info
show t1 info

port channelized-ds3

port channelized-ds3 *slot/port*

Purpose

Enters port configuration mode for the specified port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port channelized-ds3** command to configure a channelized DS-3 port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first channelized DS-3 port on the module in slot 6 of the chassis and enters port configuration mode. The port is subsequently enabled using the **no shutdown** command.

```
[local]RedBack(config)#port channelized-ds3 6/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

show bert

show bert *slot/port t1-channel*

Purpose

Shows bit error rate test (BERT) results for a T1 channel on a channelized DS-3 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and port number of the port being tested.
t1-channel	T1 channel on a channelized DS-3 port being tested.

Default

None

Usage Guidelines

Use the **show bert** command to show BERT results for a T1 channel on a channelized DS-3 port.

Examples

The following shows output for slot 4, port 1, T1 channel 1:

```
[local]RedBack#show bert 4/1 1

FRI MAY 29 03:36:07 2048
BERT stats for port 4/1, t1 1
Time test started: MAY 29 03:25:19   type of pattern: 0s
Interval selected: 1 minutes    Test is completed
Total bits received: 92154210   Total errors received: 0
```

Related Commands

bert
clear bert

show hdlc-channel counters

show hdlc-channel counters [*slot/port* [**hdlc-channel** *chan-name*]]

Purpose

Displays the statistics for one or more High-level Data Link Control (HDLC) channels.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number for a channelized DS-3 port.
hdlc-channel *chan-name*	Optional. Name of a specific HDLC channel to be displayed.

Default

Displays statistics for all HDLC channels on the system.

Usage Guidelines

Use the **show hdlc-channel counters** command to display HDLC statistics. If no slot or port is specified, a summary of statistics for all HDLC channels is shown. If you specify a slot and port, a summary of statistics for all HDLC channels on that port is shown. If you specify a slot and port and an HDLC channel, statistics for that HDLC channel are shown.

Examples

The following is sample output from the **show hdlc-channel counters** command:

```
[local]RedBack>show hdlc-channel counters 4/0

THU FEB 11 02:56:54 2010
Slot                                                          Xmt Pkts
Port Channel Name Pkts Rcvd    Pkts Sent  Bytes Rcvd   Bytes Sent   Dropped
---- ------------ -----------  ---------- ------------ ------------ ----------
 4/0 a                  25173      177208      1762096     12404546     211576
 4/0 b                  25257      177125      1767976     12398736     189010
 4/0 c                  24767      177555      1733676     12428906     934393
 4/0 d                  24729      177606      1731926     12435836   10655695
 4/0 e                  25657      177000      1796816     12393626     171138
```

```
 4/0 f                  25862      177031      1810746     12395516     148878
 4/0 g                  25736      177379      1802066     12419946     151406
 4/0 h                  25498      177844      1785336     12452426     160422

[local]RedBack>show hdlc-channel counters 4/0 hdlc-channel e

THU FEB 11 02:57:12 2010
Port  4/0, channel e (4)
pkts rcvd:  31683               pkts sent:  218529
bytes rcvd: 2217796             bytes sent: 15297016
xmt pkts outstanding: 0         xmt pkts dropped: 171138
xmt partial pkts: 218529        unprovisioned channels: 0
xmt pkts malformed: 0           xmt pkt underflows: 0
xmt pkt aborts: 0
```

Related Commands

show hdlc-config

show hdlc-config

show hdlc-config [*slot/port* [**hdlc-channel** *chan-name*]]

Purpose

Displays configuration information about High-level Data Link Control (HDLC) ports or channels, or both.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number for a particular port.
hdlc-channel *chan-name*	Optional. Name of a specific HDLC channel on a channelized DS-3 port to be displayed. This construct is valid only for channelized DS-3 ports.

Default

Displays configuration information for all HDLC ports and channels on the system.

Usage Guidelines

Use the **show hdlc-config** command to display information about HDLC ports or channels, or both. If the *slot/port* argument is specified, the display includes more detailed information. In the case of a channelized DS-3 port, you also have the option of limiting the display to a specific HDLC channel name in addition to the slot and port.

This command displays limited information for ports configured as Frame Relay because other commands (such as **show frame-relay lmi-stats**) are available that provide more information. You can use the **show port table** command to display the state of any port.

Examples

The following example shows using the **show hdlc-config** command without any optional arguments to narrow the display:

```
[local]RedBack>show hdlc-config

MON AUG 09 16:24:19 1999
Port      Channel        Encaps         State        Binding
----      -------        ------         -------      -----
2/0                      PPP            UP           a@b
2/1                      PPP            UP           b@a
```

```
3/0                     Cisco HDLC     DOWN         a[local]
3/1                     Frame Relay    n/a          n/a
5/0       fred          Frame Relay    n/a          n/a
5/0       george        Frame Relay    n/a          n/a
```

The following example shows a specific slot and port configured as PPP:

```
[local]RedBack>show hdlc-config 2/1

MON AUG 09 16:24:51 1999
Port      Channel        Encaps         State        Binding
----      -------        ------         -------      -----
2/1                      PPP            UP           b@a
```

The following example shows a specific channel on a DS-3 port:

```
[local]RedBack>show hdlc-config 5/0 hdlc-channel fred

MON AUG 09 16:25:09 1999
Port      Channel        Encaps         State        Binding
----      -------        ------         -------      -----
5/0       fred           Frame Relay    n/a          n/a
```

The following example shows specifying a specific port configured as HDLC:

```
[local]RedBack>show hdlc-config 3/0
MON AUG 09 16:25:30 1999
Port      Channel     State   Keep Alive   MySeq   YourSeq
----      -------     ------  ----------   -----   -------
3/0                   DOWN    10           0       0
```

Related Commands

show hdlc-channel counters
show port table

show pmon

show pmon [*slot/port* {**all** | *t1-channel*}][**pm** [**tabular**] [*interval-count*]]

Purpose

Displays performance monitoring statistics for T1 channels on channelized DS-3 ports.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a channelized DS-3 port.
all	Shows performance monitoring statistics for all T1 channels on a channelized DS-3 port.
t1-channel	T1 channel for which performance monitoring statistics are displayed.
pm	Optional. Shows only performance monitoring information and no information about alarms.
tabular	Optional. Shows the performance monitoring statistics in tabular form.
interval-count	Optional. Number of intervals to display. The range of values is 1 to 96; the default is 96.

Default

Displays information for all configured E1 ports and T1 ports and channels on the system.

Usage Guidelines

Use the **show pmon** command to display performance monitoring statistics for T1 channels.

If you specify the **pm** keyword, no alarm information is shown.

If you specify the **tabular** keyword, information for 15-minute intervals is shown in a column format. If you specify the *interval-count* argument, only the performance monitoring information for that number of intervals is shown. Otherwise, information for the last 24 hours is shown.

Examples

The following example shows output for slot 6, port 4:

```
[local]RedBack#show pmon 6/0 1

TUE DEC 21 13:09:43 1999
port 6/0, t1 1
    loss of signal        :    0,
    loss of frame         :    1, last occurred DEC 16 16:46:06
    AIS alarm             :    1, current duration 4d20h
    Remote alarm          :    0,
24-hour stats (last 96 15-minute intervals):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 0 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 86400 Unavail Secs
Data in current interval (549 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 0 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 549 Unavail Secs
Data in Interval 1 (start at 13:00:34):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 0 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs
Data in Interval 2 (start at 12:45:34):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 0 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs
Data in Interval 3 (start at 12:30:34):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 0 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs
             .
             .
             .
```

The following example shows performance-monitoring output in tabular format:

```
[local]RedBack#show pmon 6/0 1 pm tabular

TUE DEC 21 13:11:19 1999
port 6/0, t1 1
Interval        LCV  PCV  LOFC  LES  PES PESB  SES  UAS
 1) 13:00:35      0    0     0    0    0    0    0  900
 2) 12:45:35      0    0     0    0    0    0    0  900
 3) 12:30:35      0    0     0    0    0    0    0  900
 4) 12:15:35      0    0     0    0    0    0    0  900
 5) 12:00:35      0    0     0    0    0    0    0  900
 6) 11:45:35      0    0     0    0    0    0    0  900
 7) 11:30:35      0    0     0    0    0    0    0  900
 8) 11:15:35      0    0     0    0    0    0    0  900
 9) 11:00:35      0    0     0    0    0    0    0  900
10) 10:45:35      0    0     0    0    0    0    0  900
```

```
11) 10:30:35      0    0     0    0    0    0    0  900
12) 10:15:35      0    0     0    0    0    0    0  900
13) 10:00:35      0    0     0    0    0    0    0  900
14) 09:45:35      0    0     0    0    0    0    0  900
15) 09:30:35      0    0     0    0    0    0    0  900
16) 09:15:35      0    0     0    0    0    0    0  900
17) 09:00:35      0    0     0    0    0    0    0  900
18) 08:45:35      0    0     0    0    0    0    0  900
19) 08:30:35      0    0     0    0    0    0    0  900
20) 08:15:35      0    0     0    0    0    0    0  900
          .
          .
          .
```

Related Commands

clear pmon

show t1 info

show t1 info *slot/port* [*channel*]

Purpose

Displays configuration information for T1 channels on channelized DS-3 ports.

Command Mode

operator exec

Syntax Description

slot/port	Backplane slot number and port number for a channelized DS-3 port.
channel	Optional. T1 channel number on a channelized DS-3 port.

Default

Displays information for all T1 channels on a channelized DS-3 port.

Usage Guidelines

Use the **show t1 info** command to display information on one or more T1 channels on a channelized DS-3 port. If you omit the channel argument, all T1 channels are displayed.

Examples

The following example shows sample output from the **show t1 info** command for slot 6, port 1, T1 channel 1:

```
[local]RedBack>show t1 info 6/1 1

T1 1:
    fdl                         = off
    framing                     = esf
    out of frame                = 2 of 6
    clock-source                = internal
    linecode                    = b8zs
    yellow-alarm detection      = on
    yellow-alarm generation     = on
    loopback                    = none
```

Related Commands

show port info

speed

speed {**56** | **64**}

default speed

Purpose

Sets the speed for all the DS-0 channels in the High-level Data Link Control (HDLC) channel.

Command Mode

HDLC channel configuration

Syntax Description

56	Specifies that the DS-0 speed is 56 kbps.
64	Specifies that the DS-0 speed is 64 kbps.

Default

The default is 64 kbps.

Usage Guidelines

Use the **speed** command to configure the speed for all the DS-0 channels in the HDLC channel.

Use the **default** form of this command to configure the DS-0 channels to use the default speed.

Examples

The following example sets the DS-0 speed to 56 kbps:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#hdlc-channel 1 t1 1
[local]RedBack(config-chan)#speed 56
```

Related Commands

hdlc-channel

t1

t1 *t1-channel*

Purpose

Selects a constituent T1 channel and enters T1 channel configuration mode.

Command Mode

port configuration

Syntax Description

t1-channel	Number of the T1 channel you want to configure. The range of values is 1 to 28.

Default

None

Usage Guidelines

Use the **t1** command to configure a T1 channel on a channelized DS-3 port. This command enters T1 channel configuration mode.

Examples

The following example shows enters T1 configuration mode to configure the fourth T1 channel:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#t1 4
[local]RedBack(config-t1)#
```

Related Commands

show port info
show t1 info

yellow-alarm

yellow-alarm {**detection** | **generation**}

no yellow-alarm {**detection** | **generation**}

default yellow-alarm {**detection** | **generation**}

Purpose

Enables the detection or generation of a yellow alarm on the T1 channel.

Command Mode

T1 channel configuration

Syntax Description

detection	Enables yellow-alarm detection.
generation	Enables yellow-alarm generation.

Default

Detection and generation of a yellow alarm are enabled by default.

Usage Guidelines

Use the **yellow-alarm** command to enable the detection or generation of yellow alarms on a T1 channel.

Use the **default** form of this command to set the specified yellow alarm function back to the default value.

Use the **no** form of this command to disable the specified yellow alarm function.

Examples

The following example shows enabling yellow alarm detection on a T1 channel:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#t1 3
[local]RedBack(config-t1)#yellow-alarm detection
```

Related Commands

show port info
show t1 info

Clear-Channel DS-3 and Clear-Channel E3 Port Commands

This chapter describes the commands used to configure and maintain clear-channel DS-3 and clear-channel E3 ports through the Access Operating System (AOS).

The commands described in Chapter 9, "Common Port, Circuit, and Channel Commands," also apply to clear-channel DS-3 and clear-channel E3 ports, except where specifically noted.

If you configure a clear-channel DS-3 or clear-channel E3 port for Frame Relay encapsulation (see the **encapsulation** command), the commands described in Chapter 18, "Frame Relay Commands," also apply.

For overview information, a description of the tasks used to configure these ports, and configuration examples, see the "Configuring Clear-Channel DS-3 and Clear-Channel E3 Ports" chapter in the *Access Operating System (AOS) Configuration Guide*.

clock-source

clock-source {**internal** | **line**}

default clock-source {**internal** | **line**}

Purpose

Changes the source of the transmit data clock on a clear-channel DS-3 or E3 port.

Command Mode

port configuration

Syntax Description

internal	Specifies that the transmit clock is generated internally by the port.
line	Specifies that the transmit clock is derived from the received clock.

Default

The transmit clock is generated internally by the port.

Usage Guidelines

Use the **clock-source** command to select the source of the transmit data clock on a port.

Use the **default** form of this command to set the clock source to internal.

Examples

The following example sets the transmit clock to be derived from the received clock for a specific port:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#clock-source line
```

Related Commands

show port info

encapsulation

encapsulation {**cisco-hdlc** | **frame-relay** | **ppp**}

default encapsulation

Purpose

Sets the encapsulation type for clear-channel DS-3 and clear-channel E3 ports.

Command Mode

port configuration

Syntax Description

cisco-hdlc	Sets the encapsulation type to Cisco High-level Data Link Control (HDLC) (Cisco's proprietary HDLC encapsulation of IP) or other higher layer protocol.
frame-relay	Sets the encapsulation type to Frame Relay.
ppp	Specifies the encapsulation type as RFC 1662, *PPP in HDLC-like Framing*.

Default

The encapsulation type is Frame Relay.

Usage Guidelines

Use the **encapsulation** command to configure the encapsulation type for a clear-channel DS-3 or clear-channel E3 port.

The port commands that are available depend on the encapsulation type specified by this command. For example, if you configure the encapsulation as Cisco HDLC, none of the Frame Relay commands described in Chapter 18, "Frame Relay Commands" are available.

Use the **default** form of this command to set the encapsulation type to the default, Frame Relay.

Examples

The following example specifies PPP encapsulation on a DS-3 port and binds subscriber `george` in the local context:

```
[local]RedBack(config)#port ds3 4/1
[local]RedBack(config-port)#encapsulation ppp
[local]RedBack(config-port)#bind subscriber george@local
```

Related Commands

bind authentication
bind interface
bind subscriber

framing

framing {**c-bit** | **m13**}

default framing

Purpose

Sets the framing on a clear-channel DS-3 port.

Command Mode

port configuration

Syntax Description

c-bit	Sets the framing to C-bit.
m13	Sets the framing to M13.

Default

The framing on a clear-channel DS-3 port is M13.

Usage Guidelines

Use the **framing** command to configure the framing on a clear-channel DS-3 port. This command does not apply to clear-channel E3 ports.

Use the **default** form of this command to set the framing to M13.

Examples

The following example sets the framing on the specified clear-channel DS-3 port to M13:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#framing c-bit
```

Related Commands

show port info

keepalive

keepalive *seconds*

no keepalive

default keepalive

Purpose

Sets the period in seconds between keepalives sent on the High-level Data Link Control (HDLC) channel.

Command Mode

port configuration

Syntax Description

seconds	Number of seconds between keepalives sent on the line. The range of values is 0 to 60; the default value is 10.

Default

The default number of seconds between keepalives is 10.

Usage Guidelines

Use the **keepalive** command to specify the number of seconds between keepalives sent on the port. This command is only available for ports configured with Cisco High-level Data Link Control (HDLC) encapsulation. The number of seconds must match the value configured on the interface of the router to which this line is connected.

Use the **no** form of the command to turn keepalives off so that connections are allowed to time out and terminate during periods of idleness. Specifying 0 for the *seconds* argument also has this affect.

Use the **default** form of the command to set the time between keepalives to the default value of 10 seconds.

Examples

The following example sets the time between keepalives to `20` seconds:

```
[local]RedBack(config-port)#keepalive 20
```

The following example turns keepalives off altogether:

```
[local]RedBack(config-port)#keepalive 0
```

Related Commands

encapsulation

length

length {**long** | **short**}

default length

Purpose

Specifies the length of the physical cable that is attached to a clear-channel DS-3 port.

Command Mode

port configuration

Syntax Description

long	Specifies that the cable is longer than 225 feet.
short	Specifies that the cable is 225 feet or shorter.

Default

The cable length is 225 feet or shorter.

Usage Guidelines

Use the **length** command to configure the length of the cable attached to the clear-channel DS-3 port. This command does not apply to clear-channel E3 ports.

Use the **default** form of this command to set the cable length to be 225 feet or shorter.

Examples

The following example configures the port `7/0` to operate with a cable longer than 225 feet:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#length long
```

Related Commands

show port info

loopback

loopback {**line** | **local** | **remote**}

{**no** | **default**} **loopback**

Purpose

Creates a loopback of the specified type on a port.

Command Mode

port configuration

Syntax Description

line	Configures the port such that all frames coming in on the receive line are turned around and sent back to the sender. With this option, the remote sender receives exactly what was transmitted.
local	Configures the port so that all locally generated frames are looped back to the receiver after they go through the framer.
remote	Sends the Far End Alarm and Control (FEAC) loopback command to the remote end of the line to put the remote end in loopback. Available only for DS-3 ports.

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to establish a loopback on a port. This command is typically used for testing purposes.

The **remote** keyword is only supported for clear-channel DS-3 ports. To use this keyword, you must configure the DS-3 port framing as C-bit.

Use the **no** or **default** form of this command to remove any type of loopback from the port.

Examples

The following example configures a DS-3 port to operate in `local` loopback:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#loopback local
```

Related Commands

framing
show port info

port ds3

port ds3 *slot/port*

Purpose

Enters port configuration mode for the specified clear-channel DS-3 port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port ds3** command to configure a clear-channel DS-3 port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first clear-channel DS-3 port on the module in slot 5 of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port ds3 5/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

port e3

port e3 *slot/port*

Purpose

Enters port configuration mode for the specified clear-channel E3 port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port e3** command to configure a clear-channel E3 port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first clear-channel E3 port on the module in slot `6` of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port e3 6/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

HSSI Port Commands

This chapter describes the commands used to configure and maintain High-Speed Serial Interface (HSSI) ports through the Access Operating System (AOS).

The commands described in Chapter 9, “Common Port, Circuit, and Channel Commands,” also apply to HSSI ports, except where specifically noted.

If you configure a HSSI port for Frame Relay encapsulation (see the **encapsulation** command), the commands described in Chapter 18, “Frame Relay Commands,” also apply.

For overview information, a description of the tasks used to configure HSSI ports, and configuration examples, see the “Configuring HSSI Ports” chapter in the *Access Operating System (AOS) Configuration Guide*.

encapsulation

encapsulation {**cisco-hdlc** | **frame-relay** | **ppp**}

default encapsulation

Purpose

Sets the encapsulation type for High-Speed Serial Interface (HSSI) ports.

Command Mode

port configuration

Syntax Description

cisco-hdlc	Sets the encapsulation type to Cisco High-Level Data Link Control (HDLC) (Cisco's proprietary HDLC encapsulation of IP), or other higher layer protocol.
frame-relay	Sets the encapsulation type to Frame Relay.
ppp	Sets the encapsulation type as RFC 1662, *PPP in HDLC-like Framing*.

Default

The encapsulation type is Frame Relay.

Usage Guidelines

Use the **encapsulation** command to configure the encapsulation type for HSSI ports. The commands that are available in port and HDLC channel configuration modes that are available depend upon the encapsulation type specified by this command. For example, if you specify Cisco HDLC, none of the Frame Relay commands described in Chapter 18, "Frame Relay Commands," are available.

Use the **default** form of this command to set the encapsulation type to the default, Frame Relay.

Examples

The following example specifies Point-to-Point Protocol (PPP) encapsulation on an HSSI port and binds subscriber `george` in the `local` context:

```
[local]RedBack(config)#port hssi 4/1
[local]RedBack(config-port)#encapsulation ppp
[local]RedBack(config-port)#bind subscriber george@local
```

Related Commands

bind authentication
bind interface
bind subscriber

hardware-interface

hardware-interface {**dce** | **dte**}

default hardware-interface

Purpose

Configures the hardware interface type for a High-Speed Serial Interface (HSSI) port to be either data communications equipment (DCE) or data terminal equipment (DTE).

Command Mode

port configuration

Syntax Description

dce	Configures the port to be a hardware DCE.
dte	Configures the port to be a hardware DTE.

Default

The hardware interface is DTE.

Usage Guidelines

Use the **hardware-interface** command to configure the hardware interface type for an HSSI port. The HSSI port has to present either a DCE or DTE interface to the remote end. Among other differences, if the interface is DCE, the transmit clock is derived internally, whereas if the interface is DTE, the transmit clock is derived from the receive clock.

This command has no dependency on the **frame-relay intf-type** command; this command defines the interface at the hardware level, while the **frame-relay intf-type** command defines the Local Management Interface (LMI) at a software level. Both commands can specify DCE or DTE, or they can specify the opposite of each other (for example, you can specify the hardware interface type as DCE and the Frame Relay interface type as DTE, or vice versa).

Use the **no** form of this command to set the hardware interface type to DTE.

Examples

The following example configures an HSSI port to be a hardware `DCE`:

```
[local]RedBack1(config)#port hssi 7/0
[local]RedBack1(config-port)#hardware-interface dce
```

Related Commands

frame-relay intf-type
show port info

keepalive

keepalive *seconds*

no keepalive

default keepalive

Purpose

Sets the period in seconds between keepalives sent on the line.

Command Mode

port configuration

Syntax Description

seconds	Number of seconds between keepalives sent on the line. The range of values is 0 to 60; the default value is 10.

Default

Keepalives are enabled with an interval between transmissions of 10 seconds.

Usage Guidelines

Use the **keepalive** command to configure the number of seconds between keepalives sent on the line. This command is only available when the encapsulation has been set to Cisco High-Level Data Link Control (HDLC). The number of seconds must match the value configured on the interface of the router to which this line is connected.

Use the **no** form of this command turns keepalives off so that connections are allowed to time out and terminate during periods of idleness. Specifying 0 for the *seconds* argument also has this effect.

Use the **default** form of this command to set the period between keepalives to the default value of 10 seconds.

Examples

The following example sets the period between keepalives to `20` seconds:

```
[local]RedBack(config-port)#keepalive 20
```

The following example turns keepalives off altogether:

```
[local]RedBack(config-port)#keepalive 0
```

Related Commands

encapsulation

loopback

loopback {**internal** | **local**}

{**no** | **default**} **loopback**

Purpose

Creates a loopback of the specified type on a High-Speed Serial Interface (HSSI) port.

Command Mode

port configuration

Syntax Description

internal	Configures the port so that all locally generated frames are looped back to the receiver internally in the DSCC4.
local	Configures the port so that all locally generated frames are looped back to the receiver after they go through the DSCC4.

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to establish a loopback on the port. This command is typically used for testing purposes.

The **internal** keyword is available only on HSSI ports with the hardware interface configured as data communications equipment (DCE).

Use the **no** or **default** form of this command to remove any type of loopback from the port.

Examples

The following example configures an HSSI port to operate in `local` loopback:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#loopback local
```

Related Commands

hardware-interface
show port info

port hssi

port hssi *slot/port*

Purpose

Enters port configuration mode to configure the specified High-Speed Serial Interface (HSSI) port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port hssi** command to enter port configuration mode to configure a HSSI port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first HSSI port on the module in slot 3 of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port hssi 3/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

Packet T1 and Packet E1 Port Commands

This chapter describes the commands used to configure and maintain packet T1 and packet E1 ports through the Access Operating System (AOS).

The commands described in Chapter 9, “Common Port, Circuit, and Channel Commands,” also apply to packet T1 and packet E1 ports, except where specifically noted.

If you configure a packet T1 or packet E1 port for Frame Relay encapsulation (see the **encapsulation** command), the commands described in Chapter 18, “Frame Relay Commands,” also apply.

For overview information, a description of the tasks used to configure packet T1 and packet E1 ports, and configuration examples, see the “Configuring Packet T1 and Packet E1 Ports” chapter in the *Access Operating System (AOS) Configuration Guide*.

bert

bert *slot/port* **pattern** {**2^15** | **2^20** | **2^23** | **0s** | **1s**} **interval** *minutes*

no bert *slot/port*

Purpose

Enables bit error rate test (BERT) on the specified physical T1 or E1 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and the specific port number on a particular module.
pattern	Specifies the test data pattern.
2^15	Specifies a 2^15 test pattern.
2^20	Specifies a 2^20 test pattern.
2^23	Specifies a 2^23 test pattern.
0s	Specifies all zeros as the test pattern.
1s	Specifies all ones as the test pattern.
interval *minutes*	Number of minutes to run testing.

Default

None

Usage Guidelines

Use the **bert** command to begin bit error rate testing. To check the test results, use the **show bert** administrator exec command.

Use **no** form of this command to disable testing.

Examples

The following command enables testing on port `5/1`, using a test pattern of all zeros, for `10` minutes:

```
[local]RedBack#bert 5/1 pattern 0s interval 10
```

Related Commands

clear bert
loopback
show bert

cablelength

cablelength {**long** {**0db** | **-7.5db** | **-15db** | **-22.5db**} | **short** {**110** | **220** | **330** | **440** | **550** | **660**}}

default cablelength

Purpose

Specifies the length of the attached T1 cable or the transmit output power.

Command Mode

port configuration

Syntax Description

long	Indicates a long cable (over 660 feet).
0db	Specifies a transmit power level of 0 decibels.
-7.5db	Specifies a transmit power level of -7.5 decibels.
-15db	Specifies a transmit power level of -15 decibels.
-22.5db	Specifies a transmit power level of -22.5 decibels.
short	Indicates a short cable (up to 660 feet).
110	Specifies a cable length of up to 110 feet.
220	Specifies a cable length of up to 220 feet.
330	Specifies a cable length of up to 330 feet.
440	Specifies a cable length of up to 440 feet.
550	Specifies a cable length of up to 550 feet.
660	Specifies a cable length of up to 660 feet.

Default

None

Usage Guidelines

Use the **cablelength** command to specify the length of the attached cable, and the transmit power level. This command does not apply to packet E1 ports.

When you use the **short** keyword, the length specified indicates that the cable is equal to or less than the specified value. For example, the command **cablelength short 440** means that the cable is between 331 and 440 feet. When you use the **long** keyword, you must also specify the transmit power level.

Use the **default** form of this command to return the settings to the default values.

Examples

The following example configures the port to operate with a cable that is between `331` and `440` feet in length:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#cablelength short 440
```

Related Commands

show port info

clear bert

clear bert *slot/port*

Purpose

Clears bit error rate test (BERT) counters for a T1 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and port number of the port being tested.

Default

None

Usage Guidelines

Use the **clear bert** command to clear BERT counters for a T1 port.

Examples

The following example shows output for slot 4, port 1:

```
[local]RedBack#clear bert 4/1
```

Related Commands

bert
show bert

clear pmon

clear pmon *slot/port* [**-noconfirm**]

Purpose

Clears all performance monitoring information for an E1 port or T1 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and port number of the port.
-noconfirm	Optional. Specifies that no confirmation prompt appears before the command is run.

Default

None

Usage Guidelines

Use the **clear pmon** command to clear all performance monitoring information for an E1 or T1 port.

Examples

The following example clears the performance monitoring information for all T1 port `5/0`:

```
[local]RedBack#clear pmon 5/0 -noconfirm
```

Related Commands

show pmon

clock-source

clock-source {**internal** | **line**}

default clock-source

Purpose

Specifies the source for the transmit clock for the T1 or E1 framer.

Command Mode

port configuration

Syntax Description

internal	Specifies the onboard clock as the source.
line	Specifies the derived receive clock as the source.

Default

The transmit clock uses the onboard clock (internal) as its source.

Usage Guidelines

Use the **clock-source** command to specify the source of the transmit clock for the T1 or E1 framer.

Use the **default** form of this command to set the source to internal.

Examples

The following example sets the source for the transmit clock to the derived receive clock:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#clock-source line
```

Related Commands

show port info

encapsulation

encapsulation {**cisco-hdlc** | **frame-relay** | **ppp**}

default encapsulation

Purpose

Sets the encapsulation type for packet T1 and packet E1 ports.

Command Mode

port configuration

Syntax Description

cisco-hdlc	Specifies the encapsulation type as Cisco High-level Data Link Control (HDLC) (Cisco's proprietary HDLC encapsulation of IP) or other higher layer protocol.
frame-relay	Specifies the encapsulation type as Frame Relay.
ppp	Specifies the encapsulation type as RFC 1662, *PPP in HDLC-like Framing*.

Default

The encapsulation type is Frame Relay.

Usage Guidelines

Use the **encapsulation** command to command to configure the encapsulation type for the port.

Use the **default** form of this command to set the encapsulation type to the default of Frame Relay.

Examples

The following example specifies PPP encapsulation for a T1 port and binds subscriber `george` in the `local` context:

```
[local]RedBack(config)#port ds1 4/1
[local]RedBack(config-port)#encapsulation ppp
[local]RedBack(config-port)#bind subscriber george@local
```

Related Commands

bind authentication
bind interface
bind subscriber
keepalive

fdl

fdl {**ansi** | **att**}

no fdl

Purpose

Enables a one-second transmission of the performance report for the T1 channel using the Facility Data Link (FDL) per ANSI T1.403.

Command Mode

port configuration

Syntax Description

ansi	Enables a one-second transmission of the performance report.
att	Enables the sending of a 15-minute transmission of the performance report.

Default

Performance reports are disabled.

Usage Guidelines

Use the **fdl** command to enable the transmission of performance reports on a packet T1 port. This command applies only to Packet T1 cards configured with Extended Superframe (ESF) framing; it does not apply to packet E1 ports.

Use the **no** form of this command to disable the transmissions.

Examples

The following example enables a one-second transmission of the performance report:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#fdl ansi
```

Related Commands

framing
show port info

framing

framing {**esf** | **sf** | **crc4** | **no-crc4**}

no framing

default framing

Purpose

Selects the framing on a T1 or E1 port.

Command Mode

port configuration

Syntax Description

esf	Specifies Extended Superframe Format (ESF) for T1 ports. This option is only valid for T1 ports.
sf	Specifies Superframe Format (or D4) for T1 ports. This option is only valid for T1 ports.
crc4	Specifies CRC4 framing, per the ITU G.704 specification, for E1 ports. This option is only valid for E1 ports.
no-crc4	Specifies no CRC4 framing, per the ITU G.704 specification, for E1 ports. This option is only valid for E1 ports.

Default

T1 ports use ESF framing; E1 ports use CRC4 framing.

Usage Guidelines

Use the **framing** command to specify the framing on a packet T1 or packet E1 port.

Use the **default** form of this command to set the framing back to the default value for the port type.

Use the **no** form of this command to specify no framing, per the ITU G.704 specification. The **no** form is only available for packet E1 ports.

Examples

The following example sets the framing on a T1 port to SF:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#framing sf
```

Related Commands

show port info

invert-data

invert-data

{**no** | **default**} **invert-data**

Purpose

Inverts the polarity of all bits in the High-level Data Link Control (HDLC)-encoded data stream.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

Bits are not inverted.

Usage Guidelines

Use the **invert-data** command to invert the polarity of all bits in the HDLC-encoded data stream.

Use the **no** or **default** form of this command to return the bits in the HDLC-encoded data stream to their original polarity.

Examples

The following example inverts the polarity on the HDLC-encoded data stream on a T1 port:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#invert-data
```

Related Commands

show port info

keepalive

keepalive *seconds*

no keepalive

default keepalive

Purpose

Sets the period in seconds between keepalives sent on the line.

Command Mode

port configuration

Syntax Description

seconds	Number of seconds between keepalive messages sent on the line. The range of values is 0 to 60; the default value is 10.

Default

Keepalives are enabled with an interval between transmissions of 10 seconds.

Usage Guidelines

Use the **keepalive** command to configure the number of seconds between keepalives. This command is only available when the encapsulation has been set to Cisco High-level Data Link Control (HDLC). The number of seconds must match the value configured on the interface of the router to which the line is connected.

Use the **no** form of this command to turn keepalives off so that connections are allowed to time out and terminate during periods of idleness. Specifying a value of 0 for the *seconds* argument also has this effect.

Use the **default** form of this command to set the number of seconds between keepalives to the default value of ten seconds.

Examples

The following example sets the time between keepalives to `20` seconds:

```
[local]RedBack(config-port)#keepalive 20
```

Related Commands

encapsulation

linecode

linecode {**ami** | **b8zs**}

default linecode

Purpose

Selects the line coding for a T1 channel.

Command Mode

port configuration

Syntax Description

ami	Specifies alternate mark inversion (AMI) as the line coding.
b8zs	Specifies B8ZS as the line coding.

Default

The port uses B8ZS line coding.

Usage Guidelines

Use the **linecode** command to select the line coding for a packet T1 port. This command does not apply to packet E1 ports.

Use the **default** form of this command to set the line coding to the default of B8ZS.

Examples

The following example sets the line coding to `AMI`:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#linecode ami
```

Related Commands

show port info

loopback

loopback {**line** | **local** | **remote**}

no loopback

Purpose

Creates a loopback on the port.

Command Mode

port configuration

Syntax Description

line	Specifies that the port's receive line is looped to the transmit line.
local	Specifies that the port's transmit output is looped to the receive input.
remote	Puts the far end in loopback. Supported only for T1 ports.

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to establish a loopback of the specified type on the port. The **remote** option is valid only for packet T1 ports configured with Extended Superframe Format (ESF) framing.

Use the **no** form of this command to remove the loopback.

Examples

The following example creates a `local` loopback on a T1 port:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#loopback local
```

Related Commands

bert
framing
show port info

port ds1

port ds1 *slot/port*

Purpose

Enters port configuration mode for the specified port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port ds1** command to configure a packet T1 port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first DS-1 port on the module in slot 3 of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port ds1 3/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

port e1

port e1 *slot/port*

Purpose

Enters port configuration mode for the specified port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port e1** command to configure a packet E1 port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first E1 port on the module in slot 4 of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port e1 4/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

show bert

show bert *slot/port*

Purpose

Shows bit error rate test (BERT) results for a packet T1 or E1 port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and port number of the port being tested.

Default

None

Usage Guidelines

Use the **show bert** command to show BERT results for a packet T1 or E1 port.

Examples

The following shows output for slot 4, port 1:

```
[local]RedBack#show bert 4/1

FRI MAY 29 03:36:07 2048
BERT stats for port 4/1
Time test started:  MAY 29 03:25:19     type of pattern: 0s
Interval selected: 1 minutes    Test is completed
Total bits received: 92154210    Total errors received: 0
```

Related Commands

bert
clear bert

show pmon

show pmon [*slot/port*] [**pm** [**tabular**] [*interval-count*]]

Purpose

Displays performance monitoring statistics for packet T1 and packet E1 ports.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a Frame Relay port.
pm	Optional. Shows only performance monitoring information and no information about alarms.
tabular	Optional. Shows the performance monitoring statistics in tabular form.
interval-count	Optional. Number of intervals to display. The range of values is 1 to 96; the default is 96.

Default

Displays information for all configured E1 ports and T1 ports and channels.

Usage Guidelines

Use the **show pmon** command to display performance monitoring statistics for a port. If you specify the *slot/port* argument, the output shows only information for that slot and port.

If you specify the **pm** keyword, the output excludes alarm information.

If you specify the **tabular** keyword , the output displays information for 15-minute intervals in column format. If you specify the *interval-count* argument, the display includes only the performance monitoring information for that number of intervals. Otherwise, the display includes information for the last 24 hours.

Examples

The following example shows output for slot 6, port 4:

```
[local]RedBack>show pmon 6/4

FRI MAR 05 16:49:57 1999
port 6/4
    loss of signal        :    0,
    loss of frame         :    0,
    AIS alarm             :    0,
    Remote alarm          :    0,
24-hour stats (last 13 15-minute intervals):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 1 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (158 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations,
    0 Fr Loss Secs, 0 Line Err Secs, 0 Errored Secs,
    0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following example shows performance monitoring output in tabular format:

```
[local]RedBack>show pmon 6/4 pm tabular

FRI MAR 05 16:50:52 1999
port 6/4
Interval        LC   PCV  LOFC  LES  PES PESB  SES  UAS
 1) 13:32:15     0    0     0    1    0    0    0    0
 2) 13:47:15     0    0     0    0    0    0    0    0
 3) 14:02:15     0    0     0    0    0    0    0    0
 4) 14:17:15     0    0     0    0    0    0    0    0
 5) 14:32:15     0    0     0    0    0    0    0    0
 6) 14:47:15     0    0     0    0    0    0    0    0
 7) 15:02:15     0    0     0    0    0    0    0    0
 8) 15:17:15     0    0     0    0    0    0    0    0
 9) 15:32:15     0    0     0    0    0    0    0    0
10) 15:47:15     0    0     0    0    0    0    0    0
11) 16:02:15     0    0     0    0    0    0    0    0
12) 16:17:15     0    0     0    0    0    0    0    0
13) 16:32:15     0    0     0    0    0    0    0    0
    Total        0    0     0    1    0    0    0    0
```

Related Commands

clear pmon

show t1 info

show t1 info *slot/port*

Purpose

Displays configuration information for a T1 port.

Command Mode

operator exec

Syntax Description

slot/port	Backplane slot number and port number of a T1 port.

Default

None

Usage Guidelines

Use the **show t1 info** command to display configuration information for a T1 port.

Examples

The following example shows sample output from the **show t1 info** command:

```
[local]RedBack>show t1 info 6/1

port t1 7/1
 Loss of signal (LOS)       = no
 Loss of frame  (LOF)       = yes
 AIS alarm                  = yes
 Remote alarm               = no

 Framing                    = esf
 Clock source               = internal
 Line code                  = b8zs
 Timeslot                   = 1-24
 DS0 speed                  = 64k
 Inverted data              = no
 Yellow alarm detection     = yes
```

```
Yellow alarm generation   = yes
Facility Data Link (FDL)  = off
Cable length              = short 110
Loopback                  = none
```

Related Commands

show configuration

speed

speed {**56** | **64**}

default speed

Purpose

Sets the DS-0 or E0 speed for all DS-0 or E0 channels on the packet T1 or E1 port.

Command Mode

port configuration

Syntax Description

56	Specifies that the speed is 56 kbps.
64	Specifies that the speed is 64 kbps.

Default

The speed is 64 kbps.

Usage Guidelines

Use the **speed** command to configure the speed of the DS-0 or E0 channels.

Use the **default** form of this command to set the speed to the default of 64 kbps.

Examples

The following example sets the speed of the DS-0 channels on T1 port `4/1` to `56` kbps:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#speed 56
```

Related Commands

show port info

timeslot

timeslot *range*

default timeslot

Purpose

Defines which timeslots within the T1 or E1 port comprise the High-level Data Link Control (HDLC) channel.

Command Mode

port configuration

Syntax Description

range	Range of timeslots that comprise the HDLC channel. Hyphens and commas are allowed when specifying the range. The valid timeslots for T1 ports are 1 to 24; the valid timeslots for E1 ports are 1 to 31.

Default

The timeslots include 1 to 24 (all timeslots) for T1 ports. The timeslots include 1to 15 and 17 to 31 for E1 ports.

Usage Guidelines

Use the **timeslot** command to define the timeslots that comprise the HDLC channel.

For E1 ports, timeslot 16 is excluded unless you explicitly include it using the **ts16** command.

Use the **default** form of this command to set the timeslot range to the default of 1-24 (T1) or 1-15, 17-31 (E1). Note that when you use the **default** command for E1 ports, timeslot 16 is removed from the port configuration. You must use the **ts16** command to reconfigure timeslot 16.

Examples

The following example specifies that timeslots `1` through `12` comprise the HDLC channel on a T1 port:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#timeslot 1-12
```

The following example specifies that timeslots `1` through `20` comprise the HDLC channel on an E1 port. The **ts16** command is used to include timeslot `16`:

```
[local]RedBack(config)#port e1 5/0
```

```
[local]RedBack(config-port)#timeslot 1-20
[local]RedBack(config-port)#ts16
```

Related Commands

show port info
ts16

ts16

ts16

no ts16

Purpose

Specifies that timeslot 16 is to be included in the E1 High-level Data Link Control (HDLC) channel.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

Timeslot 16 is excluded from the E1 channel.

Usage Guidelines

Use the **ts16** command to include timeslot 16 in the E1 HDLC channel on a packet E1 port. Timeslot 16 is excluded unless you explicitly include it using this command. This command does not apply to packet T1 ports.

Use the **no** form of this command to disable timeslot 16 on an E1 port.

Examples

The following example specifies that timeslots `1` through `20` comprise the HDLC channel on an E1 port:

```
[local]RedBack(config)#port e1 5/0
[local]RedBack(config-port)#timeslot 1-20
[local]RedBack(config-port)#ts16
```

Related Commands

show port info
timeslot

yellow-alarm

yellow-alarm {**detection** | **generation**}

no yellow-alarm {**detection** | **generation**}

default yellow-alarm {**detection | generation**}

Purpose

Enables the detection or generation of yellow alarms on a T1 or E1 channel.

Command Mode

port configuration

Syntax Description

detection	Enables detection of yellow alarms.
generation	Enables generation of yellow alarms.

Default

Detection and generation of a yellow alarm are enabled.

Usage Guidelines

Use the **yellow-alarm** command to enable the detection or generation of yellow alarms on a packet T1 or packet E1 port.

Use the **no** form of this command to disable detection or generation of yellow alarms.

Use the **default** form of this command to enable detection or generation of yellow alarms.

Examples

The following example enables both `yellow-alarm detection` and `generation`:

```
[local]RedBack(config)#port ds1 4/0
[local]RedBack(config-port)#yellow-alarm detection
[local]RedBack(config-port)#yellow-alarm generation
```

Related Commands

show port info

Packet over SONET Port Commands

This chapter describes the commands used to configure and maintain Packet over Synchronous Optical Network (POS) ports supported through the Access Operating System (AOS).

The commands described in Chapter 9, “Common Port, Circuit, and Channel Commands,” also apply to POS ports, except where specifically noted.

If you configure a POS port for Frame Relay encapsulation (see the encapsulation command), the commands described in Chapter 18, “Frame Relay Commands” also apply.

For overview information, a description of the tasks used to configure POS ports, and configuration examples, see the “Configuring Packet over SONET Ports” chapter in the *Access Operating System (AOS) Configuration Guide*.

c2byte

c2byte *value*

default c2byte

Purpose

Configures the value for the Path Signal Label (C2) byte.

Command Mode

port configuration

Syntax Description

value	Value to send in the C2 byte. The range of values is 0 to 255; the default is 22 (hexadecimal 0x16) if scrambling is enabled and 207 (hexadecimal 0xCF) if scrambling is disabled.

Default

If scrambling is enabled, the default value is 22 (hexadecimal 0x16). If scrambling is disabled, the default value is 207 (hexadecimal 0xCF).

Usage Guidelines

Use the **c2byte** command to configure the value to send in the Path Signal Label (C2) byte. RFC 2615, *PPP over SONET/SDH*, specifies that a C2 byte value of 22 (hexadecimal 0x16) is used to indicate Point-to-Point Protocol (PPP) with X^43 + 1 scrambling, and the value of 207 (hexadecimal 0xCF) is used to indicate PPP without scrambling.

Note The Access Operating System (AOS) automatically configures the C2 byte to match the values specified in RFC 2615 when you configure scrambling (see the **scramble** port configuration command). If you need to modify the C2 byte value, configure scrambling first, then modify the C2 value.

Use the **default** form of this command to set the Path Signal Label (C2) byte back to the default value.

Examples

The following example configures the port to use the value `22` (hexadecimal value `0x16`) in the C2 byte:

```
[local]RedBack(config-port)#c2byte 22
```

Related Commands

scramble
show port info

clock-source

clock-source {**internal** | **line**}

default clock-source

Purpose

Changes the source of the transmit data clock on a port.

Command Mode

port configuration

Syntax Description

internal	Specifies that the transmit clock is generated internally by the port.
line	Specifies that the transmit clock is derived from the received clock.

Default

The transmit clock is generated internally by the port.

Usage Guidelines

Use the **clock-source** command to configure the source of the transmit clock on a port.

Use the **default** form of this command to set the clock source to internal.

Examples

The following example sets the transmit clock to be derived from the received clock for a specific port:

```
[local]RedBack(config)#port pos 7/0
[local]RedBack(config-port)#clock-source line
```

Related Commands

show port info

crc16

crc16

default crc16

Purpose

Enables a 16-bit cyclic redundancy check (CRC) on the port.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

A 32-bit CRC is used.

Usage Guidelines

Use the **crc16** command to configure a 16-bit CRC on a Packet over SONET (POS) OC-3 port configured with either STS-3 (Synchronous Optical Network [SONET]) or SDH framing.

Note We recommend a A 32-bit CRC.

Use the **default** form of this command to configure the port for a 32-bit CRC.

Examples

The following example enables a 16-bit CRC on a port:

```
[local]RedBack(config-port)#framing sdh
[local]RedBack(config-port)#crc16
```

Related Commands

framing sdh
show port info

encapsulation

encapsulation {**cisco-hdlc** | **frame-relay** | **ppp**}

default encapsulation

Purpose

Sets the encapsulation type for the Packet over Synchronous Optical Network (POS) port.

Command Mode

port configuration

Syntax Description

cisco-hdlc	Sets the encapsulation type to Cisco High-Level Data Link Control (HDLC) (Cisco's proprietary HDLC encapsulation of IP) or other higher layer protocol.
frame-relay	Sets the encapsulation type to Frame Relay.
ppp	Specifies the encapsulation type as Point-to-Point encapsulation per RFC 2615, *PPP over SONET/SDH* and RFC 1662, *PPP in HDLC-like Framing*.

Default

The encapsulation type is Frame Relay.

Usage Guidelines

Use the **encapsulation** command to configure the encapsulation type for a POS port.

The port commands that are available depend on the encapsulation type specified by this command. For example, if you specify **cisco-hdlc**, none of the Frame Relay commands described in Chapter 18, "Frame Relay Commands" are available.

Use the **default** form of this command to set the encapsulation type to the default, Frame Relay.

Examples

The following example specifies PPP encapsulation on a DS-3 port and binds subscriber `george` in the `local` context:

```
[local]RedBack(config)#port pos 4/1
[local]RedBack(config-port)#encapsulation ppp
[local]RedBack(config-port)#bind subscriber george@local
```

Related Commands

bind authentication
bind interface
bind subscriber

framing sdh

framing sdh

default framing

Purpose

Configures the framing on a Packet over SONET (POS) port to SDH.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

The port uses Synchronous Optical Network (SONET) framing.

Usage Guidelines

Use the **framing sdh** command to configure the framing for a POS port to SDH.

Use the **default** form of this command to set the framing to SONET.

Examples

The following example sets the framing on the specified port to SDH:

```
[local]RedBack(config)#port pos 7/0
[local]RedBack(config-port)#framing sdh
```

Related Commands

show port info

loopback

loopback {**diag** | **line** | **local** | **r2t** | **t2r**}

{**no** | **default**} **loopback**

Purpose

Creates a loopback of the specified type on a Packet over SONET (POS) port.

Command Mode

port configuration

Syntax Description

diag	Configures a diagnostic loopback on the serializer chip.
line	Configures a line loopback on the serializer chip.
local	Configures local loopback on the SONET framer.
r2t	Configures SONET physical interface (PHY) line loopback.
t2r	Configures SONET PHY internal loopback .

Default

Loopback is disabled.

Usage Guidelines

Use the **loopback** command to establish a loopback on the port. This command is typically used for testing purposes. The various options supported can help to isolate the source of a problem on the port. Follow these guidelines:

- To test operation of the serializer for a port, use the **diag** keyword. This option connects the transmit to the receive lines on the serializer chip.
- To test operation between the serializer and the SONET framer, use the **line** keyword. This option routes retimed serial data from the receive inputs to the transmitter outputs on the serializer.
- To test operation of the SONET framer, use the **local** keyword. This option connects the transmit queue to the receive queue at the SONET framer.
- To test operation of the SONET PHY, use the **t2r** keyword. This option connects the transmit queue to the receive queue at the SONET PHY.
- To test end-to-end operation on the line, use the **r2t** keyword. This option connects the receive queue to the transmit queue at the SONET PHY.

Use the **no** or **default** form of this command to remove any type of loopback from the port.

Examples

The following example configures a POS port to operate in `local loopback`:

```
[local]RedBack(config)#port pos 7/0
[local]RedBack(config-port)#loopback local
```

Related Commands

framing sdh
show port info

packet-length

packet-length *value*

default packet-length

Purpose

Specifies the maximum High-Level Data Link Control (HDLC) frame length for the port.

Command Mode

port configuration

Syntax Description

value	Maximum HDLC frame length in bytes. The range of values is 1,508 to 65,528; the default value is 16,384.

Default

The maximum packet length is 16,384 bytes.

Usage Guidelines

Use the **packet-length** command to configure the maximum HDLC frame length for the port.

Use the **default** form of this command to return the maximum HDLC frame length for the port back to the default value.

Examples

The following example configures the maximum frame length to be `24576`:

```
[local]RedBack(config-port)#packet-length 24576
```

Related Commands

show port info

port pos

port pos *slot/port*

Purpose

Enters port configuration mode for the specified Packet over SONET (POS) port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port pos** command to configure a POS port. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is created in the configuration.

This command does not have a **no** form. (Ports cannot be deleted.)

Examples

The following example selects the first POS port on the module in slot 3 of the chassis and enters port configuration mode. The **no shutdown** command enables the port.

```
[local]RedBack(config)#port pos 7/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

scramble

scramble

{**no** | **default**} **scramble**

Purpose

Enables payload scrambling on the port.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

Scrambling is enabled on the port.

Usage Guidelines

Use the **scramble** command to enable X^43 +1 scrambling, as specified in RFC 2615, *PPP over SONET/SDH*.

Note Enabling or disabling scrambling on a port also changes the Path Label Signal (C2) byte value to the default specified in the RFC 2615. See the **c2byte** port configuration command.

Use the **no** or **default** form of this command to disable payload scrambling.

Examples

The following example disables scrambling on port `7/0`. It also results in the C2 value being set to the default value of 0xCF.

```
[local]RedBack(config)#port pos 7/0
[local]RedBack(config-port)#no scramble
```

Related Commands

c2byte
show port info

ATM Commands

This chapter describes the commands use to configure Asynchronous Transfer Mode (ATM) features through the Access Operating System (AOS).

Chapter 11, “ATM Port Commands,” describes the commands used to configure ATM ports.

For overview information, a description of the tasks used to configure ATM features, and configuration examples, see the “Configuring ATM” chapter in the *Access Operating System (AOS) Configuration Guide*.

atm ping

atm ping {**path** | **channel**} {**segment** | **end-to-end**} *slot/port vpi* [*vci*] [**count** *number*] [**timeout** *seconds*]

Purpose

Tests Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) by sending operation, administration, and maintenance (OAM) loopback cells.

Command Mode

operator exec

Syntax Description

path	Sends F4 OAM loopback cells down the specified virtual path connection.
channel	Sends F5 OAM loopback cells down the specified virtual channel connection.
segment	Sends OAM loopback cells to a neighbor switch.
end-to-end	Sends OAM loopback cells to the end of the connection where ATM cells are terminated.
slot/port	Backplane slot number and port number of an ATM port.
vpi	Virtual path identifier (VPI). The range of values is 0 to 255.
vci	Virtual channel identifier (VCI). You must specify this argument with the **channel** keyword; you can not specify it with the **path** keyword. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
count *number*	Optional. Number of OAM cells to send. The range of values is 1 to 10000; the default is 5.
timeout *seconds*	Optional. Time in seconds that AOS waits for a response for each OAM ping. The range of values is 1 to 100; the default is 2.

Default

None

Usage Guidelines

Use the **atm ping** command to test the reachability of a neighboring ATM switch or the end of an ATM connection.

Use the **path** keyword to send F4 OAM loopback cells down a specific virtual path. To use the **path** keyword, you must first configure VCI 3 (used for path segment testing) and VCI 4 (used for path end-to-end testing).

Examples

The following example sends 16 end-to-end F5 cells on VPI:VCI `2:47` on the ATM port in slot `5`, port `0`:

```
[local]RedBack>atm ping channel end-to-end 5/0 2 47 count 16
Sending 16, end-to-end F5 cells on 5/0, 2:47, timeout is 2 seconds:
!!!!!!!!!!!!!!!!
Success rate is 100 percent (10/10)
```

Related Commands

atm pvc
loopback

atm profile

atm profile *prof-name*

no atm profile *prof-name*

Purpose

Creates an Asynchronous Transfer Mode (ATM) profile with the given name (if it does not already exist) and enters ATM profile configuration mode.

Command Mode

global configuration

Syntax Description

prof-name	Alphanumeric string to be used as the name of the particular profile.

Default

By default, no ATM profiles are defined on the system.

Usage Guidelines

Use the **atm profile** command to create or modify an ATM profile. You must create an ATM profile before you can configure ATM permanent virtual circuits (PVCs) that reference the profile name.

Use the **no** form of this command to delete an ATM profile. You cannot delete an ATM profile if any ATM PVCs reference that profile.

Examples

The following example creates an ATM profile named `low_rate` and enters ATM profile configuration mode:

```
[local]RedBack(config)#atm profile low_rate
[local]RedBack(config-atmpro)#
```

Related Commands

atm pvc
show atm profile

atm pvc

atm pvc *vpi vci* [**through** *end-vci*] **profile** *prof-name* **encapsulation** {**auto1483** | **bridge1483** | **route1483** | **dot1q** | **l2tp** [**vc-muxed**] | **multi** | **ppp** [**auto** | **over-ethernet** | **serial** | **nlpid** | **llc** | **vc-muxed**]}

no atm pvc *vpi vci* [**through** *end-vci*]

Purpose

Creates a new Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) or a range of PVCs (if it does not already exist), and enters circuit configuration mode.

Command Mode

port configuration

Syntax Description

vpi	Virtual path identifier (VPI). The range of values is 0 to 255.
vci	Virtual channel identifier (VCI). For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI in a range of similar PVCs to configure.
profile *prof-name*	Existing ATM traffic-shaping profile to use for the PVC.
encapsulation	Specifies the encapsulation type (from the keywords that follow).
auto1483	Enables the auto-detect feature with regard to choosing between RFC 1483 bridged and routed encapsulation types.
bridge1483	Indicates RFC 1483 bridged encapsulation.
route1483	Indicates RFC 1483 routed encapsulation.
dot1q	Indicates that the PVC carries 802.1Q traffic.
l2tp	Indicates that the PVC carries a Layer 2 Tunneling Protocol (L2TP) tunnel. When you use this keyword without the **vc-muxed** keyword, the Logical Link Control (LLC) Service Network Access Point (SNAP) value of L2TP is selected by default.
vc-muxed	Optional. Selects VC multiplexed as the type of L2TP encapsulation.
multi	Specifies that the circuit contains both RFC 1483 bridged and PPP over Ethernet (PPPoE) encapsulations.

ppp	Indicates Point-to-Point Protocol (PPP) encapsulation. When used alone, VC-multiplexed encapsulation is selected by default.
auto	Optional. Enables the auto-detect feature with regard to the PPP encapsulation type.
over-ethernet	Optional. Selects PPPoE encapsulation.
serial	Optional. Selects Serial (High-level Data Link Control [HDLC]) PPP encapsulation—used in non-RFC-compliant configurations.
nlpid	Optional. Selects Network Layer Protocol Identifier (NLPID) PPP encapsulation.
llc	Optional. Selects LLC/SNAP PPP encapsulation as defined in RFC 2364, *PPP over AAL5*.
vc-muxed	Optional. Selects VC multiplexed encapsulation as defined in RFC 2364. This is the default PPP encapsulation type.

Default

No ATM PVCs are defined.

Usage Guidelines

Use the **atm pvc** command to create or configure an ATM PVC or a range of ATM PVCs with similar characteristics. You can use this command to modify a subset of PVCs that have been defined with the **atm pvc explicit** and **atm pvc on-demand** commands. The ATM profile you specify must exist prior to using this command.

Use the **through** keyword to provision groups of similar PVCs on an ATM port. The following guidelines apply when you use the **through** keyword:

- Any ATM PVCs in the specified range that do not already exist are created with the specified profile and encapsulation.
- Any ATM PVCs in the specified range that do exist (including those defined with the **atm pvc explicit** and **atm pvc on-demand** commands) are modified to use the specified profile and encapsulation.
- The **bind subscriber** and **ip host** commands cannot be used in conjunction with the **atm pvc through** command. You can create a PVC range, then subsequently modify individual PVCs if use of these commands is required.
- When you use the **no** form of this command in conjunction with the **through** keyword, all ATM PVCs in the range will be deleted, regardless of whether those PVCs have the same profile and encapsulation. You can delete a subset of PVCs.

Note When you use the **through** keyword with this command, the Access Operating System (AOS) generates a single command in the configuration for each PVC in the specified range. To avoid a large configuration file, use the **atm pvc explicit** command to configure explicit PVC ranges.

When you specify the **dot1q** keyword for the encapsulation, you can create 802.1Q PVCs on the circuit.

Two forms of auto detection are possible with this command. The **auto1483** keyword enables auto detection between RFC 1483 bridged and routed encapsulations; the **ppp auto** keywords enable auto detection among the various PPP encapsulations.

When you specify the **auto1483** keyword, the circuit mode commands that become visible are the union of those available for the **bridge1483** and **route1483** keywords. The Access Operating System (AOS) handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **ip host** *ip-address* [*mac-address*] command accepts both forms (with or without the *mac-address* argument) for the **bind interface** command, and puts a message into the system log if the wrong type of command is entered for the type of encapsulation eventually detected.

When you specify the **ppp auto** keywords, the circuit mode commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. AOS handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **bind authentication** command accepts a **max-sessions** specification, which is ignored (effectively set to 1) if the encapsulation is not PPPoE.

Use the **no** form of this command to delete a previously configured PVC or range of PVCs. The **no** form of this command does not affect PVCs that have been defined with the **atm pvc explicit** or the **atm pvc on-demand** commands.

Examples

The following example creates a PVC that references a previously defined ATM profile named `dslam1`, an encapsulation of `ppp vc-muxed` (the default PPP encapsulation), and a VPI:VCI of `0:32`:

```
[local]RedBack(config)#port atm 2/0
[local]RedBack(config-port)#atm pvc 0 32 profile dslam1 encapsulation ppp
```

The next example creates 101 PVCs that all reference the previously defined ATM profile named `dslam1`, an encapsulation of `ppp vc-muxed`, and VPI:VCI values in the range of `0:32` through `0:132`:

```
[local]RedBack(config)#port atm 4/1
[local]RedBack(config-port)#atm pvc 0 32 through 132 profile dslam1 encapsulation ppp
```

The next example creates a PVC that references the previously defined ATM profile named `dslam1`, enables auto detection for the PPP encapsulation, and a VPI:VCI value of `0:32`:

```
[local]RedBack(config)#port atm 2/0
[local]RedBack(config-port)#atm pvc 0 32 profile dslam1 encapsulation ppp auto
[local]RedBack(config-pvc)#bind authentication pap max-sessions 5
```

Related Commands

atm profile
atm pvc explicit
atm pvc on-demand
bind authentication
bind interface
bind subscriber
show atm pvc

atm pvc explicit

atm pvc explicit *start-vpi:start-vci* **through** *end-vpi:end-vci* **profile** *prof-name* **encapsulation** {**auto1483** | **bridge1483** | **route1483** |**multi** | **ppp** [**auto** | **over-ethernet** | **serial** | **nlpid** | **llc** | **vc-muxed**]}

no atm pvc explicit *start-vpi:start-vci* **through** *end-vpi:end-vci*

Purpose

Sets the default profile and encapsulation and enters circuit configuration mode for an explicit range of Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

Command Mode

port configuration

Syntax Description

start-vpi	Virtual path identifier (VPI) of the first circuit in the range. The range of values is 0 to 255.
start-vci	Virtual channel identifier (VCI) of the first circuit in the range. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through	Specifies the end of the range.
end-vpi	VPI of the last circuit in the range. The range of values is 0 to 255.
end-vci	VCI of the last circuit in the range. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
profile *prof-name*	Name of the profile to be used as the default.
encapsulation	Selects the encapsulation type (from the keywords that follow).
auto1483	Enables the auto-detect feature with regard to choosing between RFC 1483 bridged and routed encapsulations.
bridge1483	Indicates RFC 1483 bridged encapsulation.
route1483	Indicates RFC 1483 routed encapsulation.
multi	Specifies that the circuit contains both RFC 1483 bridged and PPP over Ethernet (PPPoE) encapsulations.

ppp	Indicates Point-to-Point Protocol (PPP) encapsulation. When you use this keyword alone, selects VC-multiplexed encapsulation by default.
auto	Optional. Enables the auto-detect feature with regard to the PPP encapsulation type.
over-ethernet	Optional. Selects PPP over Ethernet (PPPoE) encapsulation.
serial	Optional. Selects Serial (High-level Data Link Control [HDLC]) PPP encapsulation—used in non-RFC-compliant configurations.
nlpid	Optional. Selects Network Layer Protocol Identifier (NLPID) PPP encapsulation.
llc	Optional. Selects Logical Link Control (LLC) Service Network Access Point (SNAP) PPP encapsulation as defined in RFC 2364, *PPP over AAL5*.
vc-muxed	Optional. Selects VC-multiplexed encapsulation as defined in RFC 2364. This is the default PPP encapsulation type.

Default

No explicit PVC ranges are defined.

Usage Guidelines

Use the **atm pvc explicit** command to create a range of ATM PVCs that share the same profile and encapsulation. This command generates a single command in the configuration file. You can use the **atm pvc** command to overwrite one or more of the PVCs in a range defined by the **atm pvc explicit** command.

The following guidelines apply to this command:

- You cannot overwrite PVC ranges that were previously configured with the **atm pvc explicit** or **atm pvc on-demand** commands, except if the new range completely encompasses that previous range.
- If you use this command to overwrite a PVC range that was previously defined with the **atm pvc on-demand** command, all active circuits are cleared.
- You can use the **atm pvc** command to overwrite one or more PVCs defined by the **atm pvc explicit** command. If you subsequently use the **no atm pvc** command to delete such a PVC, the PVC reverts to the **atm pvc explicit** definition.
- You cannot use the **no atm pvc** command to remove PVCs from an explicit range.
- You cannot use the **bind subscriber** and **ip host** commands in conjunction with this command. You can create a PVC range, then subsequently modify individual PVCs, if use of these commands is required.

Two forms of auto detection are possible with this command. The **auto1483** keyword enables auto detection between RFC 1483 bridged and routed encapsulations; the **ppp auto** keywords enable auto detection among the various PPP encapsulations.

When you specify the **auto1483** keyword, the circuit mode commands that become visible are the union of those available for the **bridge1483** and **route1483** keywords. The Access Operating System (AOS) handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected.

Specifically, the **ip host** *ip-address* [*mac-address*] command accepts both forms (with or without the *mac-address* argument) for the **bind interface** command, and puts a message into the system log if the wrong type of command is entered for the type of encapsulation eventually detected.

When you specify the **ppp auto** keywords, the circuit mode commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. AOS handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **bind authentication** command accepts a **max-sessions** specification, which is ignored (effectively set to 1) if the encapsulation is not PPPoE.

Use the **no** form of this command to remove the specified range of circuits. You must specify the same circuit range as specified in the **atm pvc explicit** command.

Examples

The following example creates an explicit range of `100` ATM PVCs that use the ATM profile named `adam` and `auto1483` encapsulation:

```
[local]RedBack(config-port)#atm pvc explicit 10:100 through 10:199 profile adam
encapsulation auto1483
[local]RedBack(config-pvc)#bind authentication chap pap
```

Related Commands

atm pvc
atm pvc on-demand
show atm pvc

atm pvc on-demand

atm pvc on-demand *start-vpi:start-vci* **through** *end-vpi:end-vci* {**profile** *prof-name* **encapsulation** {**auto1483** | **bridge1483** | **route1483** | **multi** | **ppp** [**auto** | **over-ethernet** | **serial** | **nlpid** | **llc** | **vc-muxed**]} | **aaa context** *ctx-name* [**prefix-string** *text*]}

no atm pvc on-demand *start-vpi:start-vci* **through** *end-vpi:end-vci*

Purpose

Creates a range of Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs) that will be configured automatically as activity is detected on the circuits.

Command Mode

port configuration

Syntax Description

start-vpi	Virtual path identifier (VPI) of the first circuit in the range. The range of values is 0 to 255.
start-vci	Virtual channel identifier (VCI) of the first circuit in the range. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through	Specifies the end of the range.
end-vpi	VPI of the last circuit in the range. The range of values is 0 to 255.
end-vci	VCI of the last circuit in the range. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535
profile *prof-name*	Name of the profile to be used as the default.
encapsulation	Selects the encapsulation type (from the keywords that follow).
auto1483	Enables the auto-detect feature with regard to choosing between RFC 1483 bridged and routed encapsulations.
bridge1483	Indicates RFC 1483 bridged encapsulation.
route1483	Indicates RFC 1483 routed encapsulation.
multi	Specifies that the circuit contains both RFC 1483 bridged and PPP over Ethernet (PPPoE) encapsulations.

ppp	Indicates Point-to-Point Protocol (PPP) encapsulation. When you use this keyword alone, selects VC-multiplexed encapsulation by default.
auto	Optional. Enables the auto-detect feature with regard to the PPP encapsulation type.
over-ethernet	Optional. Selects PPP over Ethernet (PPPoE) encapsulation.
serial	Optional. Selects serial (High-level Data Link Control [HDLC]) PPP encapsulation—used in non-RFC-compliant configurations.
nlpid	Optional. Selects Network Layer Protocol Identifier (NLPID) PPP encapsulation.
llc	Optional. Selects Logical Link Control (LLC) Service Network Access Point (SNAP) PPP encapsulation as defined in RFC 2364, *PPP over AAL5*.
vc-muxed	Optional. Selects VC multiplexed encapsulation as defined in RFC 2364. This is the default PPP encapsulation type.
aaa	Specifies that the circuits are created using RADIUS.
context *ctx-name*	Name of the context in which the RADIUS servers configured are used for AAA configuration.
prefix-string *text*	String to be used as a prefix in constructing the User-Name attribute. Must not contain spaces, periods, underscores, or forward/backward slashes.

Default

No on-demand PVC ranges are defined.

Usage Guidelines

Use the **atm pvc on-demand** command to create a range of PVCs that will be configured automatically as activity is detected on the circuits.

The following guidelines apply to this command:

- You cannot use this command to overwrite PVC ranges that were previously configured with the **atm pvc explicit** or **atm pvc on-demand** commands, except if the new range completely encompasses that previous range.
- If you use this command to overwrite a PVC range that was previously defined with the **atm pvc explicit** command, the circuits are not cleared. You must use the **clear circuit** command to manually clear these circuits.
- You can use the **atm pvc** command to overwrite one or more PVCs defined by this command. If you subsequently delete such a PVC with the **no atm pvc** command, the PVC reverts to the **atm pvc on-demand** definition.
- You cannot use the **no atm pvc** command to remove PVCs from an on-demand range.
- You cannot use the **bind subscriber** and **ip host** commands in conjunction with this command. You can create a PVC range, then subsequently modify individual PVCs if use of these commands is required.

Two forms of auto detection are possible with this command. The **auto1483** keyword enables auto detection between RFC 1483 bridged and routed encapsulations; the **ppp auto** keywords enable auto detection among the various PPP encapsulations.

When you specify the **auto1483** keyword, the circuit mode commands that become visible are the union of those available for the **bridge1483** and **route1483** keywords. The Access Operating System (AOS) handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **ip host** *ip-address* [*mac-address*] command accepts both forms (with or without the *mac-address* argument) for the **bind interface** command, and puts a message into the system log if the wrong type of command is entered for the type of encapsulation eventually detected.

When you specify the **ppp auto** keywords, the circuit mode commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. AOS handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **bind authentication** command accepts a **max-sessions** specification, which is ignored (effectively set to 1) if the encapsulation is not PPPoE.

When you create a range of on-demand ATM PVCs, you can use the **profile** and **encapsulation** keywords to specify the profile and encapsulation type explicitly. Alternately, you can use the **aaa** keyword to configure AOS to use RADIUS to configure the profile, encapsulation, and binding of the circuits in the range. If you use the **aaa** keyword, you must specify the context that the RADIUS server(s) is defined in with the **context** *ctx-name* construct. You can also define a prefix string that is used to construct the User-Name attribute. By default, the RADIUS User-Name is in the form *hostname.port.slot.vpi.vci*. If you define a prefix string, the RADIUS User-Name attribute is in the form *prefix-string.vpi.vci*. When you use the **aaa** keyword, this command does enter circuit configuration mode.

Use the **no** form of this command to remove the specified range of circuits. You must specify the same circuit range as specified in the **atm pvc on-demand** command.

Examples

The following example defines a range of on-demand ATM PVCs using the RADIUS servers in the `local` context to configure the PVCs when activity is detected on the circuit(s), and specifying a prefix string of `lec1-OC3`:

```
[local]RedBack(config-port)#atm pvc on-demand 100:100 through 100:999 aaa context local
prefix-string lec1-OC3
[local]RedBack(config-port)#
```

Related Commands

atm pvc
atm pvc explicit

buffers

buffers transmit *value*

default buffers transmit

Purpose

Limits the total number of outbound transmit packet buffers that can be consumed by any circuit referencing this Asynchronous Transfer Mode (ATM) profile.

Command Mode

ATM profile configuration

Syntax Description

value	Transmit queue size in number of buffers. The range of values is 1 to 1,280; the default is 50.

Default

The transmit queue size is 50 buffers.

Usage Guidelines

Use the **buffers** transmit command to configure the number of buffers for the transmit queue for all circuits that reference this profile. This command can also be applied to a port (see the **buffers** command in port configuration mode).

Caution Improper setting of this value can have severe consequences on overall system performance.

Use the **default** form of this command to return the profile to use a transmit queue size of 50 buffers.

Examples

The following example limits the transmit buffer size to `20` packets for each circuit that is configured to use the ATM profile named `test`:

```
[local]RedBack(config)#atm profile test
[local]RedBack(config-atmpro)#buffers transmit 20
```

Related Commands

buffers—port configuration mode

bulkstats schema

bulkstats schema *schema-name* **format** *format-string* [*AOS-variable* [*AOS-variable* …]]

no bulkstats schema *schema-name*

Purpose

Defines the statistics schema for the contents of the bulkstats collection file for any circuit referencing this Asynchronous Transfer Mode (ATM) profile.

Command Mode

ATM profile configuration

Syntax Description

schema-name	Name of the schema. The name can be no more than 19 characters in length.
format *format-string*	String used to format the output of the schema. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. Table 17-1 describes the supported special-character sequences.
AOS-variable	Variable for which data will be collected. An Access Operating System (AOS) variable replaces its associated *format-string* definition. Separate the variables with a space. Table 17-2 lists the AOS variables available in ATM profile configuration mode.

Table 17-1 C Programming Language printf() Syntax

Syntax	Description
%s	Character string
%d	Integer in decimal (base 10)
%u	Unsigned integer in decimal (base 10)
%x	Integer in hexadecimal format (base 16)
%%	Single % character
\n	UNIX newline character

Table 17-2 AOS Variables

AOS Variable	Type	Description
slot	Integer	Slot number in the SMS device
port	Integer	Port number on the I/O module
description	String	Description of port
sysuptime	Integer	System uptime in seconds
inoctets	Integer	Number of octets received on this circuit
outoctets	Integer	Number of octets sent from this circuit
inpackets	Integer	Number of packets received on this circuit
outpackets	Integer	Number of packets sent on this circuit
mcast_inoctets	Integer	Number of multicast octets received on this circuit
mcast_outoctets	Integer	Number of multicast octets sent on this circuit
mcast_inpackets	Integer	Number of multicast packets received on this circuit
mcast_outpackets	Integer	Number of multicast packets sent on this circuit

Default

None

Usage Guidelines

Use the **bulkstats schema** command to define the statistics schema for the contents of the bulkstats collection file for any circuit referencing this profile. You can configure multiple schemas, each gathering a different type and format of data. However, you should restrict the use of multiple schemas to global data collection and create only one schema per port, circuit, or profile. Otherwise, you may apply a profile with several schemas to a large number of circuits, slowing down the SMS processor function.

If you want to generate multiple collections of bulk statistics for a single port, circuit, or profile, create one schema designed to record separate groups of distinct data using the **\n** character sequence after each subset entry to create a new starting line.

When you define multiple schemas in a configuration mode, each of the schemas is used to create a text record that is appended to the bulkstats collection file each sample period. Every line created always has the same schema name as the first field and has a newline appended as a record separator.

Use the **no** form of this command to remove the named bulkstats schema from the ATM profile.

Examples

The following example displays an ATM profile bulkstats schema:

```
[local]RedBack(config-atmpro)#bulkstats schema example format "atm:%u, slot:%u,
port:%u, vpi:%u, vci:%u, inoct:%u, outoct: %u,” sysuptime slot port vpi vci inoctets
outoctets
```

The previous example creates a line in the collection file that looks like the following:

```
host1: atm:348765, slot:3, port:1, vpi:16, vci:233, inoct:234975, outoct:165444
```

Related Commands

bulkstats collection

clock mode

clock mode {**common** | **independent**}

default clock mode

Purpose

Sets the transmit clock mode for the inverse multiplexing over ATM (IMA) group.

Command Mode

IMA group configuration

Syntax Description

common	Specifies that all ports in the group will use a common transmit clock (CTC) source.
independent	Specifies that each port in the group will use an independent clocking (ITC) source.

Default

The default clock mode is common.

Usage Guidelines

Use the **clock mode** command to set the transmit clock mode for the IMA group. This command applies only to Asynchronous Transfer Mode (ATM) T1 IMA ports.

If you specify the clock mode as **common**, all ports in the IMA group are clocked from the same source, as specified by the **clock source** IMA group configuration command. If you specify the **independent** keyword, each port uses the clock source as specified by the **clock-source** port configuration command.

Use the **default** form of this command to set the transmit clock mode to the default value.

Examples

The following example configures all ports in the IMA group to use independent clock sources:

```
[local]RedBack(config-ima)#clock mode independent
```

Related Commands

clock source—IMA group configuration mode
clock-source—port configuration mode
show ima group

clock source

clock source {**internal** | **line** [*slot/port*]}

default clock source

Purpose

Selects the common transmit clock source for all ports in the inverse multiplexing over ATM (IMA) group.

Command Mode

IMA group configuration

Syntax Description

internal	Specifies that the common transmit clock source is the onboard oscillator.
line	Specifies the common transmit clock derived from the receive clock on a port in the group.
slot/port	Optional. Backplane slot and port number of the port in the IMA group to provide the source clock. If you do not specify this argument, the lowest numbered port in the group provides the source clock.

Default

The group uses the internal clock for the transmit clock source.

Usage Guidelines

Use the **clock source** command to configure the source clock for an IMA group. This command only applies if you configure the IMA group to use a common clock source (see the **clock mode** IMA group configuration command). Otherwise, this command has no effect.

If you specify the **line** keyword, all ports will use a transmit clock derived from the receive clock on the specified port. The specified port must be defined as a constituent of the IMA group.

Use the **default** form of this command to set the transmit clock source for the IMA group back to the default value.

Examples

The following example configures all ports in the IMA group to use the transmit clock derived from the receive clock on slot 4, port 0:

```
[local]RedBack(config-ima)#clock source line 4/0
```

Related Commands

clock source
clock-source—Port configuration mode
show ima group

clpbit

clpbit

no clpbit

Purpose

Sets the cell loss priority (CLP) bit in all cells transmitted over circuits referencing this Asynchronous Transfer Mode (ATM) profile.

Command Mode

ATM profile configuration

Syntax Description

This command has no keywords or arguments.

Default

The CLP bit is not set.

Usage Guidelines

Use the **clpbit** command to set the CLP bit in all cells transmitted over circuits that reference this profile.

Use the **no** form of this command to configure a profile that clears the CLP bit in all circuits referencing that profile.

Example

The following example adds the **clpbit** command to an ATM traffic profile named `low_rate`. All cells transmitted over circuits that reference this profile will have the CLP bit set.

```
[local]RedBack(config)#atm profile low_rate
[local]RedBack(config-atmpro)clpbit
```

Related Commands

show atm profile

counters

counters [**l2** | **multicast**]

{**no** | **default**} **counters**

Purpose

Enables statistics to be collected for circuits referencing this Asynchronous Transfer Mode (ATM) profile.

Command Mode

ATM profile configuration

Syntax Description

l2	Optional. Enables statistics collection for layer 2 packets.
multicast	Optional. Enables statistics collection for multicast (layer 3) traffic.

Default

Statistics are not collected.

Usage Guidelines

Use the **counters** command to enable the collection of statistics on circuits that reference this profile. Statistics are not collected by default because of the potentially large amount of memory needed. If memory usage is a problem, disable unnecessary multicast counters on circuits.

Use the **counters** command with no parameters specified to enable statistics collection for both layer 2 packets and multicast (layer 3) traffic. To enable statistics collection for only layer 2 packets, specify the **l2** keyword. To enable statistics collection for only multicast traffic, specify the **multicast** keyword.

For the **aaa accounting** command, accounting packets will only include packet and byte counts for a given circuit if **counters** are enabled in the ATM profile referenced by that circuit.

To obtain multicast statistics, Internet Group Management Protocol (IGMP) proxy must be enabled on the interface and context to which the circuit is bound. See the **ip multicast-routing** context configuration command, the **ip igmp** interface configuration command, the **ip multicast send** and **ip multicast receive** subscriber configuration commands, and the **router-igmp-interface** IGMP proxy router configuration command.

Use the **no** or **default** form of this command to disable statistics collection for circuits that reference this profile.

Examples

The following example configures an ATM profile named `low_rate` to enable statistics collection for both layer 2 packets and multicast (layer 3) traffic on all circuits that reference the profile.

```
[local]RedBack(config)#atm profile low_rate
[local]RedBack(config-atmpro)#counters
```

Related Commands

aaa accounting
ip igmp
ip multicast-routing
ip multicast receive
ip multicast send
router-igmp-interface
show atm counters
show atm multicast
show atm profile

debug atm

debug atm *slot/port* **pvc** *vpi vci*

no debug atm *slot/port* **pvc** *vpi vci*

Purpose

Enables debugging for a specific Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC).

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot and port number of an ATM port.
pvc	Specifies debugging on a particular PVC.
vpi	Virtual path identifier (VPI). The range of values is 0 to 255.
vci	Virtual channel identifier (VCI). For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.

Default

Debugging is disabled for all ATM PVCs.

Usage Guidelines

Use the **debug atm** command to enable debugging messages for a specific ATM PVC. This command prints the packet header and 60 bytes of payload data for all packets received and sent on the PVC.

Note The **debug all** command does not enable ATM debugging.

Use the **no** form of this command to disable debugging for a specific ATM PVC.

Examples

The following example enables ATM debugging on port 3/0, for VPI:VCI x:

```
[local]RedBack#debug atm 3/0 pvc 0 100
```

The following output displays sample messages displayed when you enable ATM debugging:

```
ATM 3/0(O) VPI:0 VCI:100
SAP:aaaa CTL:03 OUI:000000 TYPE:0800 Length:0x64
4500 0064 c094 0000 ff01 f6ff 0101 0101 0101 0102 0800 64ab 6e20 0000 0000
3623 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213 1415 1617 1819 1a1b 1c1d 1e1f

ATM 3/0(I) VPI:0 VCI:100
SAP:aaaa CTL:03 OUI:000000 TYPE:0800 Length:0x64
4500 0064 c095 0000 4001 b5ff 0101 0102 0101 0101 0000 6cab 6e20 0000 0000
3623 0405 0607 0809 0a0b 0c0d 0e0f 1011 1213 1415 1617 1819 1a1b 1c1d 1e1f
```

The first line of each message contains the slot and port, an input (I) or output (O) indicator, the VPI, and the VCI. The second line of each message in the example contains RFC 1483 encapsulation information. The remaining lines contain 60 bytes of payload data.

Related Commands

show atm pvc

delay-tolerance

delay-tolerance *time*

default delay-tolerance

Purpose

Specifies the receive inverse multiplexing over ATM (IMA) differential delay tolerance.

Command Mode

IMA group configuration

Syntax Description

time	Differential delay tolerance, in milliseconds. The range of values is 0 to 100; the default is 25ms.

Default

The delay tolerance is 25 ms.

Usage Guidelines

Use the **delay-tolerance** command to specify the receive IMA differential delay tolerance, in milliseconds.

Use the **default** form of this command to set the delay tolerance back to the default value.

Examples

The following example sets the delay tolerance for the IMA group to `50`:

```
[local]RedBack(config-ima)#delay-tolerance 50
```

Related Commands

show ima group

description

description *text*

no description

Purpose

Defines a textual description for the inverse multiplexing over ATM (IMA) group.

Command Mode

IMA group configuration

Syntax Description

text	Textual description for the IMA group. Length cannot exceed one line.

Default

No description is defined for the IMA group.

Usage Guidelines

Use the **description** command to associate additional information with an IMA group.

Use the **no** form of this command to delete a previously created description. To change a description, simply create a new one and it will overwrite the existing one.

Examples

The following example sets a description for the IMA group:

```
[local]RedBack(config-ima)#description DSL feed from Provider X
```

Related Commands

show ima group

frame-length

frame-length {**32** | **64** | **128** | **256**}

default frame-length

Purpose

Sets the frame length for the inverse multiplexing over ATM (IMA) group.

Command Mode

IMA group configuration

Syntax Description

32	Specifies a frame length of 32 bytes.
64	Specifies a frame length of 64 bytes.
128	Specifies a frame length of 128 bytes.
256	Specifies a frame length of 256 bytes.

Default

The default frame length is 128 bytes.

Usage Guidelines

Use the **frame-length** command to configure the frame length for an IMA group. You cannot change the frame length for an IMA group after you have enabled the group.

Use the **default** form of this command to set the frame length for the IMA group to the default value.

Examples

The following example sets the frame length for the IMA group to 64 bytes:

```
[local]RedBack(config-ima)#frame-length 64
```

Related Commands

ima enable
show ima group

ima enable

ima enable *group-id*

no ima enable *group-id*

Purpose

Enables the specified inverse multiplexing over ATM (IMA) group.

Command Mode

global configuration

Syntax Description

group-id	IMA group identifier. The range of values is 0 to 255.

Default

IMA groups are disabled.

Usage Guidelines

Use the **ima enable** command to enable an IMA group. You must complete all configuration for an IMA group prior to entering this command.

Use the **no** form of this command to disable an IMA group.

Examples

The following example enables IMA group 3:

```
[local]RedBack(config)#ima enable 3
```

Related Commands

ima group
show ima group

ima group

ima group *group-id*

no ima group *group-id*

Purpose

Creates the specified inverse multiplexing over ATM (IMA) group if it does not already exist, and enters IMA group configuration mode.

Command Mode

global configuration

Syntax Description

group-id	IMA group identifier. The range of values is 0 to 255.

Default

No IMA groups are defined.

Usage Guidelines

Use the **ima group** command to create and configure an IMA group. After you create and configure an IMA group, you must configure IMA parameters, then use the **ima enable** global configuration command to enable the group.

Use the **no** form of this command to delete an IMA group. The **no** form removes all information previously configured for the IMA group.

Examples

The following example creates IMA group 3:

```
[local]RedBack(config)#ima group 3
[local]RedBack(config-ima)#
```

Related Commands

ima enable
show ima group

minimum-links

minimum-links *count*

default minimum-links

Purpose

Specifies the minimum number of ports in the inverse multiplexing over ATM (IMA) group that must be active for the IMA group to be up.

Command Mode

IMA group configuration

Syntax Description

count	Minimum number of ports that must be active for the IMA group to be up. The range of values is 1 to the number of ports defined in the group.

Default

The minimum number of active ports is 1.

Usage Guidelines

Use the **minimum-links** command to specify the minimum number of ports that must be active for the IMA group to be up.

Use the **default** form of this command to set the minimum number of links to the default value.

Examples

The following example sets the minimum number of links to 3:

```
[local]RedBack(config-ima)#minimum-links 3
```

Related Commands

ports
show ima group

ports

ports *slot/port* [*slot/port* ...] **pvc-config** *slot/port*

no ports *slot/port* [*slot/port* ...]

Purpose

Defines the ports that constitute the inverse multiplexing over ATM (IMA) group and specifies which port defines the permanent virtual circuits (PVCs) for the group.

Command Mode

IMA group configuration

Syntax Description

slot/port	Backplane slot number and port number. You can specify one or more ports.
pvc-config *slot/port*	Backplane slot number and port number of the port that defines the PVCs for the IMA group.

Default

No ports are defined in the IMA group.

Usage Guidelines

Use the **ports** command to specify the ports that constitute an IMA group. The ports you define in the IMA group must be in the same slot. Also, the slot and port specified for the **pvc-config** keyword must be one of the ports defined in the IMA group. When you add a port to an IMA group and do not specify that port as the pvc configuration port, all PVCs for that port are unbound and removed from the configuration.

Use the **no** form of this command to remove one or more ports from the IMA group. When you remove a port from the IMA group, all PVCs for the port are removed from the configuration. You must reconfigure the PVCs and bindings for the port. You cannot remove the port that you defined as the pvc configuration port from the IMA group.

Examples

The following example adds three ports to the IMA group, and specifies the PVCs defined for port `4/2` are used for the IMA group:

```
[local]RedBack(config-ima)#ports 4/0 4/1 4/2 pvc-config 4/2
```

Related Commands

atm pvc
show ima group

radius attribute medium-type

radius attribute medium-type {**dsl** | **cable** | **wireless** | **satellite**}

{**no** | **default**} **radius attribute medium-type**

Purpose

Specifies the value that the Access Operating System (AOS) supplies for the Medium-Type vendor-specific attribute (VSA) in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets.

Command Mode

ATM profile configuration

Syntax Description

dsl	Specifies that the value of the Medium-Type VSA is DSL.
cable	Specifies that the value of the Medium-Type VSA is cable.
wireless	Specifies that the value of the Medium-Type VSA is wireless.
satellite	Specifies that the value of the Medium-Type VSA is satellite.

Default

Sending of the Medium-Type attribute is disabled.

Usage Guidelines

Use the **radius attribute medium-type** command to specify the value of the Medium-Type attribute for any circuits that reference the profile.

Use the **no** or **default** form of this command to disable the sending of the attribute.

Examples

The following example creates the ATM profile named `DSL-UBR` with the Medium-Type attribute configured for `dsl`. If RADIUS Accounting is enabled, then the circuits in port 4/0 that reference this profile will have Accounting packets with the Medium-Type attribute containing the value `dsl`. Similarly, attempts to authenticate the Point-to-Point (PPP) user via RADIUS will cause the attribute to be present in Access-Request packets.

```
[local]RedBack(config)#atm profile DSL-UBR
[local]RedBack(config-atmpro)#shaping ubr
```

```
[local]RedBack(config-atmpro)#radius attribute medium-type dsl
[local]RedBack(config-atmpro)#exit
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#atm pvc 0 1 through 100 profile DSL-UBR encapsulation ppp
[local]RedBack(config-pvc)#bind authentication chap pap
```

Related Commands

aaa accounting

shaping

shaping {**cbr rate** *rate* **cdv** *cdv* | **gfr mcr** *mcr* **scr** *scr* **bt** *bt* | **ubr** | **vbr-nrt pcr** *pcr* **cdvt** *cdvt* **scr** *scr* **bt** *bt* | **vbr-rt pcr** *pcr* **cdvt** *cdvt* **scr** *scr* **bt** *bt*}

default shaping

Purpose

Indicates the corresponding quality of service (QoS) traffic shaping to use for any circuit referencing this Asynchronous Transfer Mode (ATM) profile.

Command Mode

ATM profile configuration

Syntax Description

cbr	Specifies traffic shaping based on a constant bit rate (CBR).
rate *rate*	Bit rate in kbps. The range of values is 64 to 155,520.
cdv *cdv*	Cell delay variation (CDV), defined as the maximum cell delay (in ms) between the expected arrival time and the actual arrival time. The range of values is 0 to 10,000.
gfr	Specifies traffic shaping based on a guaranteed frame rate (GFR). This keyword is available only for ATM Version 2 I/O modules.
scr *scr*	Sustained cell rate (SCR), defined as the rate (in kbps) that should be maintained during transmission of cells across a particular ATM connection. The range of values is 64 to 155,520.
bt *bt*	Burst tolerance (BT), defined as the number of cells (in ms) that can be transferred back-to-back without forcing a break. The range of values is 1 to 10,000.
mcr *mcr*	Minimum cell rate (MCR), defined as the rate that should be guaranteed on a GFR channel (in kbps). The range of values is 64 to 155,520.
ubr	Configures traffic shaping based on an unspecified bit rate (UBR).
vbr-nrt	Configures traffic shaping based on variable bit rate-nonrealtime (VBR-nrt).
pcr *pcr*	Peak cell rate (PCR), an upper limit on traffic (in kbps), that can be applied to an ATM connection. The range of values is 64 to 155,520.
cdvt *cdvt*	Cell delay variation tolerance (CDVT), defined as the difference (in ms) between the cell's expected arrival time and the actual arrival time. The range of values is 0 to 10,000.

vbr-rt	Configures traffic shaping based on variable bit rate-realtime (VBR-rt).

Default

UBR shaping is configured.

Usage Guidelines

Use the **shaping** command to define the traffic shaping for circuits referencing this profile. This command must be present within the definition of an ATM profile. Successive **shaping** commands replace the previous **shaping** configuration for the profile.

Use the **default** form of this command to return the profile shaping to the default of UBR.

Examples

The following example configures an ATM traffic profile named `low_rate` with traffic shaping set to VBR-nrt traffic with a peak cell rate of 2.5 Mbps; a cell delay variation tolerance of 20 ms; a sustained cell rate of 2.4 Mbps; and a burst tolerance of 10 ms:

```
[local]RedBack(config)#atm profile low_rate
[local]RedBack(config-atmpro)#shaping vbr-nrt pcr 2500 cdvt 20 scr 2400 bt 10
```

Related Commands

atm pvc
show atm profile
show ima group

show atm counters

show atm counters [**all**] [**profile** *prof-name*] [*slot/port* [*vpi* [*vci* [**through** *end-vci*]]]] [**details** [**errors**] | **no-counters** | **summary** [**errors**]]

Purpose

Displays a list of traffic counters for configured Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

Command Mode

operator exec

Syntax Description

all	Optional. Displays information for all configured PVCs. This option is only available to operators and administrators in the local context.
profile *prof-name*	Optional. Name of an ATM profile.
slot/port	Optional. Backplane slot number and port number of an ATM port.
vpi	Optional. Virtual path identifier (VPI). The range of values is 0 to 255.
vci	Optional. Virtual channel identifier (VCI). For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when displaying counters for a range of circuits.
details	Optional. Displays more details for each PVC.
summary	Optional. Displays only a summary of bound and unbound PVCs.
errors	Optional. Displays only PVCs that have nonzero error counters.
no-counters	Optional. Displays only PVCs that do not have counters enabled.

Default

Displays the counters for all configured ATM PVCs that are bound in the current context.

Usage Guidelines

Use the **show atm counters** command to display a list of traffic counters for ATM PVCs. Per-VC traffic statistics are not kept by the system by default. See the **counters** command in ATM profile configuration mode to enable statistics collection.

In the local context, specify the **all** keyword to show all configured ATM PVCs, including both bound PVCs (any context) and unbound PVCs. In any other context, the display includes only PVCs that are bound within the current context.

If you specify a profile name, the output only displays PVCs configured with that profile.

If you specify the slot and port, the output only displays PVCs configured on that slot and port.

If you specify the VPI number, the output only displays PVCs configured with that VPI. If you also specify a VCI, the output only displays that PVC. If you specify the **through** keyword, the output displays the specified range of VCIs.

If you specify the **summary** keyword, the output only displays a summary; it does not include per-PVC counters.

If you specify the **details** keyword, the display includes detailed output for each specified PVC; otherwise, it displays one line of output for each PVC.

If you specify the **no-counters** keyword, the output only displays the PVCs that do not have counters enabled.

If you specify the **errors** keyword, the output only displays the PVCs with errors.

You can use the optional keywords in different combinations to show PVCs that interest you. For example, the **show atm counters profile atm-1 2/0 2 20 through 30 details** command displays detailed counter information for VCIs 20 through 30 on port 2/0 and VPI 2 that were configured with a profile of `atm-1` in the current context. If the `atm-1` profile does not have any counters enabled, the output displays no PVCs.

Examples

The following example displays traffic counters for all configured PVCs:

```
[local]RedBack>show atm counters all

MON JUL 26 18:08:32 1999
Slot                                                                Xmt Pkts
Port  VPI VCI   Pkts Rcvd  Pkts Sent   Bytes Rcvd   Bytes Sent  Dropped
----  --- ---   ---------  ---------   ----------   ---------- --------
 4/0    1   1           1          1           52           52        0
 4/0    2  16           5          5           86           86        0
 4/0    2  20           0          9            0          189        0
 4/0    2  21           0          9            0          189        0
 4/0    2  22           0          9            0          189        0
 4/0    4   4           0          1            0           52        0
 4/1    1   1           0          1            0           52        0
 4/1    1  17           0          0            0            0        0
 4/1    1  18           0          0            0            0        0
 4/1    1  19           0          0            0            0        0
 4/1    2  16           5          5           86           86        0
```

```
 4/1    4   4           0          1            0           52        0

pvcs with counters:        12          pvcs without counters: 0
pkts rcvd:  11           pkts sent:  41             dropped:  0
bytes rcvd: 224                  bytes sent: 947
OAM cells rcvd:  0               OAM cells sent:  0
```

The following example displays counters for slot 4, port 0:

```
[local]RedBack>show atm counters 4/0

MON JUL 26 18:08:34 1999
Slot                                                              Xmt Pkts
Port  VPI VCI  Pkts Rcvd  Pkts Sent   Bytes Rcvd  Bytes Sent    Dropped
----  --- ---- ---------  ---------   ----------  ----------   --------
 4/0    1    1         1          1           52          52          0
 4/0    2   16         5          5           86          86          0
 4/0    2   20         0          9            0         189          0
 4/0    2   21         0          9            0         189          0
 4/0    2   22         0          9            0         189          0
 4/0    4    4         0          1            0          52          0

pvcs with counters: 6            pvcs without counters: 0
pkts rcvd:  6                    pkts sent:  34               dropped:0
bytes rcvd: 138                  bytes sent: 757
OAM cells rcvd:  0               OAM cells sent:  0
```

The following example displays the output for a specific circuit:

```
[local]RedBack>show atm counters all 4/0 2 16

Slot/Port: 4/1  VPI: 2  VCI: 16  profile: joe
status: UP     bound to b@a
first created: MON JUL 26 17:02:50 1999
status change: MON JUL 26 17:02:56 1999
last cleared:  never
pkts rcvd:  5                    pkts sent:  5             dropped:0
bytes rcvd: 86                   bytes sent: 86
OAM cells rcvd:  0               OAM cells sent:  0
xmt ovfl errs: 0                 xmt null sbd info errs: 0
rcv length errs: 0               xmt crc errs:  0
rcv timeout errs: 0
```

Related Commands

counters
show atm multicast
show atm profile
show atm pvc

show atm multicast

show atm multicast [**all**] [**profile** *prof-name*] [*slot/port* [*vpi* [*vci* [**through** *end-vci*]]]] [**no-counters** | **summary** | **details**]

Purpose

Displays counters for multicast traffic on configured Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

Command Mode

operator exec

Syntax Description

all	Optional. Displays information for all configured PVCs. This option is only available to operators and administrators in the local context.
profile *prof-name*	Optional. Name of an ATM profile.
slot/port	Optional. Backplane slot number and port number of an ATM port.
vpi	Optional. Virtual path identifier (VPI). The range of values is 0 to 255.
vci	Optional. Virtual channel identifier (VCI). For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when displaying counters for a range of circuits.
summary	Optional. Displays only a summary of bound and unbound PVCs.
details	Optional. Displays more details for each PVC.
no-counters	Optional. Displays only PVCs that do not have counters enabled.

Default

Displays the multicast counters for all configured ATM PVCs that are bound within the current context.

Usage Guidelines

Use the **show atm multicast** command to display counters for multicast traffic on configured ATM PVCs. Per-VC traffic statistics are not kept by the system by default. See the **counters** command in ATM profile configuration mode to enable statistics collection.

In the local context, use the **all** keyword to show all configured ATM PVCs, including both bound PVCs (any context) and unbound PVCs. In any other context, the output includes only PVCs that are bound within the current context.

If you specify a profile name, the output only displays PVCs that reference that profile.

If you specify the *slot/port* argument, the output only displays PVCs configured on that slot and port.

If you specify the *vpi* argument, the display includes only PVCs configured with that VPI. If you also specify the *vci* argument, the display includes only that PVC. If you use the **through** keyword, the display includes the specified range of VCIs.

If you specify the **summary** keyword, the display includes only a summary; it does not include per-PVC counters.

If you specify the **details** keyword, the display includes detailed output for each specified PVC; otherwise, the display includes abbreviated output for each PVC.

If you specify the **no-counters** keyword, the output only displays the PVCs that do *not* have counters enabled.

You can use the optional keywords in different combinations to show PVCs that interest you. For example, the **show atm multicast profile atm-1 2/0 2 20 through 30 details** command displays detailed multicast counter information for VCIs 20 through 30 on port 2/0 and VPI 2 that were configured with a profile of atm-1 in the current context. If profile `atm-1` has no multicast counters enabled, the display does not show any PVCs.

Examples

The following example displays multicast statistics for all ATM PVCs bound in the local context:

```
[local]RedBack>show atm multicast

TUE JUL 06 22:20:50 1999
Slot           Multicast   Multicast  Multicast   Multicast
Port VPI  VCI  Pkts Rcvd   Pkts Sent  Bytes Rcvd  Bytes Rcvd
---- ---  ---  ---------   ---------  ----------  ----------
4/0    1    1          2           0          56           0
4/0    1    2          2           0          56           0

pvcs with mcast counters: 2   pvcs without mcast counters: 5
multicast pkts rcvd: 4        multicast pkts sent: 0
multicast bytes rcvd: 102     multicast bytes sent: 0
```

The following example displays multicast statistics for slot/port 4/0, VPI 1, VCI 1:

```
[local]RedBack>show atm multicast 4/0 1 1

TUE JUL 06 22:21:30 1999

Slot/Port: 4/0 VPI: 1  VCI: 1  profile:mcast
status: UP bound to a01@recv
first created: TUE JUL 06 22:03:09 1999
status change: TUE JUL 06 22:21:24 1999
last cleared:  never
multicast pkts rcvd: 3        multicast pkts sent: 0
multicast bytes rcvd: 84      multicast bytes sent:0
```

The following example displays detailed multicast statistics for all PVCs bound in the local context:

```
[local]RedBack>show atm multicast details

Slot/Port: 4/0 VPI: 1  VCI: 1  profile:mcast
status: UP bound to a01@recv
first created: THU JAN 01 00:00:00 1999
status change: THU JUL 22 01:32:59 1999
last cleared:  never
multicast pkts rcvd: 3       multicast pkts sent: 0
multicast bytes rcvd: 84     multicast bytes sent:0

Slot/Port: 4/0 VPI: 1  VCI: 2  profile:mcast
status: UP bound to a02@recv
first created: THU JAN 01 00:00:00 1999
status change: THU JUL 22 01:32:59 1999
last cleared:  never
multicast pkts rcvd: 3       multicast pkts sent: 0
multicast bytes rcvd: 84     multicast bytes sent:0

THU JUL 22 01:38:08 1999
pvcs with mcast counters:2   pvcs without mcast counters: 0
multcast pkts rcvd:6         multicast pkts sent: 0
multicast bytes rcvd:168     multicast bytes sent: 0
```

The following example displays a brief summary of multicast statistics:

```
[local]RedBack>show atm multicast summary

THU JUL 22 01:38:53 1999
pvcs with mcast counters:2   pvcs without mcast counters: 0
multcast pkts rcvd:8         multicast pkts sent: 0
multicast bytes rcvd:224     multicast bytes sent: 0
```

Related Commands

counters
show atm counters
show atm profile
show atm pvc

show atm profile

show atm profile [*prof-name*]

Purpose

Displays Asynchronous Transfer Mode (ATM) traffic management parameters.

Command Mode

operator exec

Syntax Description

prof-name	Name of a configured ATM profile.

Default

Displays a list of all configured ATM profiles.

Usage Guidelines

Use the **show atm profile** command to display information on an ATM profile. If the you do not include the optional *prof-name* argument, the output includes the traffic management parameters for all defined ATM profiles. Otherwise, the output only displays parameters for the specified profile.

Examples

The following example displays sample output from the **show atm profile** command:

```
[local]RedBack>show atm profile

MON AUG 09 14:00:02 1999
                                Xmt  CLP CBR CBR  CBR
Name     Schedule Mode  Cntr  Buf  Bit Pri Rate CDV PCR CDVT SCR BT
-------- -------------  ----  ---  --- --- ---- --- --- ---- --- --
mcast    ubr            l2mc  def    0
```

The counters field (Cntr) can indicate:

- none—the profile specified no counters
- l2—the profile specified layer 2 counters
- mc—the profile specified multicast counters
- l2mc—the profile specified both layer 2 and multicast counters

Related Commands

counters
shaping

show atm pvc

show atm pvc [**all**] [**profile** *prof-name*] [*slot/port* [*vpi* [*vci* [**through** *end-vci*]]]] [**summary** | **up** | **down**]

Purpose

Displays a list of configured Asynchronous Transfer Mode (ATM) permanent virtual circuits (PVCs).

Command Mode

operator exec

Syntax Description

all	Optional. Displays all configured PVCs. This option is available only to operators and administrators in the local context.
profile *prof-name*	Optional. Name of an ATM profile.
slot/port	Optional. Backplane slot number and port number of an ATM port.
vpi	Optional. Virtual path identifier (VPI) of an ATM PVC. The range of values is 0 to 255.
vci	Optional. Virtual channel identifier (VCI) of an ATM PVC. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when displaying counters for a range of circuits.
summary	Optional. Displays only summary information.
up	Optional. Displays only active PVCs.
down	Optional. Displays only inactive PVCs.

Default

Displays all configured ATM PVCs that are bound within the current context.

Usage Guidelines

Use the **show atm pvc** command to display a list of configured ATM permanent virtual circuits.

In the local context, use the **all** keyword to display all configured ATM PVCs, including both bound PVCs (any context) and unbound PVCs. The **all** keyword is only available in the local context. In any other context, the output includes only PVCs that are bound within the current context.

If you specify a profile name, the output only displays PVCs configured with that profile.

If you specify the *slot/port* argument, the output only displays PVCs configured on that slot and port.

If you specify the *vpi* argument, the output only displays PVCs configured with that VPI. If you also specify the *vci* argument, the output only displays that PVC. If you use the **through** keyword, the output includes the specified range of VCIs.

For any PVCs configured with an auto-detection encapsulation (encapsulation type set to **ppp auto** or **auto1483**), the output shows the PVC encapsulation type as **auto** *type* until the actual encapsulation type has been detected. Once the encapsulation type has been detected, the output displays the specific Point-to-Point Protocol (PPP) or RFC 1483 bridged encapsulation type.

If you use the **summary** keyword, the output includes only a summary; it does not display per-PVC counters.

If you specify the **up** keyword, the output only displays active PVCs.

If you specify the **down** keyword, the output only displays inactive PVCs.

Examples

The following example displays all configured PVCs:

```
[local]RedBack>show atm pvc all

MON AUG 9 14:22:02 1999
Port  VPI  VCI  Traffic Profile State Ctrs Encaps     Binding
----  ---  ---  --------------- ----- ---- ---------- -------
 4/0    1    1  ubr              UP   l2   bridge1483 atm50@atm
 4/0    2   16  joe              UP   l2   ppp        a@b
 4/0    2   20  ubr              UP   l2   ppp
 4/0    2   21  ubr              UP   l2   ppp
 4/0    2   22  ubr              UP   l2   ppp
 4/0    4    4  ubr              UP   l2   bridge1483 atm40@atm
 4/1    1    1  ubr2             UP   l2   multi      atm51@atm2
 4/1    1   17  ubr              UP   l2   route1483
 4/1    1   18  ubr              UP   l2   bridge1483
 4/1    1   19  ubr              UP   l2   route1483
 4/1    2   16  joe              UP   l2   ppp        b@a
 4/1    4    4  ubr2             UP   l2   bridge1483 atm41@atm
 4/1    1    1  mcast            UP   l2mc route1483  a01@recv
 4/1    1    2  mcast            UP   l2mc route1483  a02@recv
circuits up: 14  circuits down: 0  total circuits: 14
```

The counters column (Ctrs) can indicate:

- none—no counters were specified in the profile
- l2—**counters l2** (layer 2) was specified in the profile
- mc—**counters multicast** was specified in the profile
- l2mc—both **l2** and **multicast** were specified in the profile

The following example displays a specific circuit:

```
[local]RedBack>show atm pvc 4/1 1 1

Slot/Port: 4/1  VPI: 1  VCI: 1  profile: ubr2
status: UP     bound to atm51@atm2
first created: SAT AUG 09 10:28:33 1999
status change: SAT AUG 09 12:09:33 1999
last cleared:  never
pkts rcvd:  1                 pkts sent:  2           dropped:0
bytes rcvd: 52                bytes sent: 104
OAM cells rcvd:  0            OAM cells sent:  0
xmt ovrfl errs:  0            xmt null sbd info errs: 0
rcv length errs: 0            rcv crc errs:    0
rcv timeout errs: 0
```

Related Commands

atm profile
atm pvc
counters
show atm profile

show ima group

show ima group [*group-id*]

Purpose

Displays inverse multiplexing over ATM (IMA) group configuration and status information.

Command Mode

operator exec

Syntax Description

group-id	Optional. IMA group identifier. The range of values is 0 to 255.

Default

Displays information for all configured IMA groups.

Usage Guidelines

Use the **show ima group** command to display summary IMA group information for all IMA groups. To display more detailed information about a single IMA group, use the *group-id* argument.

Examples

The following example displays IMA group information for all configured IMA groups:

```
[local]RedBack>show ima group

GRP-ID   GRP_ENAB  GRP_STATE   CLK_MODE   PVC_PORT  TOTAL_LINK  LINK_UP
 10       Yes        Up          CTC        4/0        3           1
 20       Yes        Up          CTC        4/1        1           1
 30       No         Down        CTC        --         0           0
```

The following example displays IMA group information for IMA group `10`:

```
[local]RedBack>show ima group 10

group id         :  0
group status     :  enable
group pvc port   :  port 0
clock mode       :  ctc
clock source     :  internal
maximum delay    :  5 milliseconds
```

```
symmetry          :  symmetric config / symmetric operation
frame length      :  128
minimum link      :  1
group links       :  port 0, port 2, port 3,
total links       :  3
```

Related Commands

ima enable
ima group
show ima pmon

show ima pmon

show ima pmon *group-id* [*slot/port*] [**pm** [**tabular**] [*interval*]]

Purpose

Displays inverse multiplexing over ATM (IMA) group information.

Command Mode

operator exec

Syntax Description

group-id	IMA group identifier. The range of values is 0 to 255.
slot/port	Optional. Backplane slot number and port number.
pm	Optional. Displays only performance monitoring information and no information about alarms.
tabular	Optional. Displays performance monitoring statistics in tabular form.
interval	Optional. Number of intervals to be displayed. The range of values is 1 to 96; the default is 1.

Default

Displays performance monitoring and alarm information for all ports in an IMA group.

Usage Guidelines

Use the **show ima pmon** command to display performance monitoring and alarm information for an IMA group, or for a specific port within an IMA group.

Examples

The following example displays performance monitoring information for IMA group `10`:

```
[local]RedBack>show ima pmon 10

THU SEP 02 22:52:02 1999
    fe start up stage       :  1, last occurred SEP 02 20:34:35
    ne abort configuration  :  0,
    fe abort configuration  :  0,
    ne insufficient links   :  1, last occurred SEP 02 20:34:39
    fe insufficient links   :  1, last occurred SEP 02 20:34:39
```

```
    fe blocked state        :  1, last occurred SEP 02 20:34:22
    ne/fe timing mismatch   :  0,
    fe unavailable status   :  0,
24-hour group id=10 stats (last 2 15-minute intervals):
    2 Group NE Fail number,1 Group FE Fail number,
    17 Group Unavailable Seconds ,0 Group Tx Cell Rate,
    0 Group Rx Cell Rate
Group id=10 data in current interval (166 seconds elapsed):
    0 Group NE Fail number,0 Group FE Fail number,
    0 Group Unavailable Seconds ,3591 Group Tx Cell Rate,
    3591 Group Rx Cell Rate
```

The following example displays performance monitoring information for IMA group `10`, port `4/0`:

```
[local]RedBack>show ima pmon 10 port 4/0

THU SEP 02 22:55:17 1999
 loss of IMA frame          :  1, last occurred SEP 02 20:34:35
 link out of delay sync     :  0,
 Tx link mis-connected      :  0,
 remote link failure        :  0,
 link fault                 :  1,
 fe tx unusable             :  0,
 fe rx unusable             :  0,
24-hour link num=0 stats (last 9 15-minute intervals):
 5 ICP cell violations,4 NE severely error seconds,
 0 NE unavailable seconds,0 NE Tx unusable seconds,
 10 NE Rx unusable seconds,0 NE Tx failure numbers,
 0 NE Rx failure numbers,3 OIF anomalies numbers,
 14322 Tx cell stuff events,14313 Rx cell stuff events,
 2 FE severely error seconds,0 FE unavailable seconds,
 0 FE Tx unusable seconds,0 FE Rx unusable seconds,
 0 FE Tx failure numbers,0 FE Rx failure numbers
Link num=0 data in current interval (361 seconds elapsed):
 0 ICP cell violations,0 NE severely error seconds,
 0 NE unavailable seconds,0 NE Tx unusable seconds,
 0 NE Rx unusable seconds,0 NE Tx failure numbers,
 0 NE Rx failure numbers,0 OIF anomalies numbers,
 639 Tx cell stuff events,639 Rx cell stuff events,
 0 FE severely error seconds,0 FE unavailable seconds,
 0 FE Tx unusable seconds,0 FE Rx unusable seconds,
 0 FE Tx failure numbers,0 FE Rx failure numbers
```

The following example displays tabular performance monitoring information only for IMA group `10`, port `4/0`:

```
[local]RedBack>show ima pmon 10 port 4/0 pm tabular

THU SEP 02 22:57:20 1999
group id 10/ slot4 port0
Interval        ICPV      NESES   NEUAS   OIF   FESES   FEUAS
1) 20:34:15       2         4       0      1      1       0
2) 20:57:15       1         0       0      1      1       0
```

```
3) 21:12:15       2         0       0       1       0       0
4) 21:27:15       0         0       0       0       0       0
5) 21:42:15       0         0       0       0       0       0
6) 21:57:15       0         0       0       0       0       0
7) 22:12:15       0         0       0       0       0       0
8) 22:27:15       0         0       0       0       0       0
9) 22:42:15       0         0       0       0       0       0
Total             5         4       0       3       2       0
```

Related Commands

ima enable
ima group
show ima group

symmetry

symmetry configuration {**symmetric** | **asymmetric**} **operation** {**symmetric** | **asymmetric**}

default symmetry

Purpose

Defines the configuration and operation symmetry parameters for the inverse multiplexing over ATM (IMA) group.

Command Mode

IMA group configuration

Syntax Description

configuration	Specifies whether or not a different number of links can be configured in each direction.
symmetric	Specifies that the same number of links must be configured in each direction.
asymmetric	Specifies that the same number of links are not required in each direction.
operation	Specifies whether or not a link can be used to forward traffic, even if the link has failed in the reverse direction.
symmetric	Specifies that the link cannot be used to forward traffic if the link has failed in the reverse direction.
asymmetric	Specifies that the link can be used to forward traffic, even if the link has failed in the reverse direction.

Default

The default is symmetric configuration and symmetric operation.

Usage Guidelines

Use the **symmetry** command to set the configuration and operation symmetry parameters for an IMA group. You can not specify symmetric operation with asymmetric configuration. You cannot change the symmetry parameters for an IMA group after you have enabled the IMA group.

Use the **default** form of this command to set the configuration and operation symmetry parameters to the default values.

Examples

The following command configures the IMA group for symmetric configuration and symmetric operation:

```
[local]RedBack(config-ima)#symmetry configuration symmetric operation symmetric
```

Related Commands

ima enable
show ima group

Frame Relay Commands

This chapter describes the commands used to configure and maintain Frame Relay ports and features supported by the Access Operating System (AOS). The configuration commands described in this chapter apply only to ports or channels that have been configured with Frame Relay encapsulation.

For overview information, a description of the tasks used to configure Frame Relay features, and configuration examples, see the "Configuring Frame Relay" chapter in the *Access Operating System (AOS) Configuration Guide*.

buffers

buffers transmit *value*

{**default**} **buffers transmit**

Purpose

Limits the total number of outbound transmit-packet buffers that can be used by a circuit referencing this Frame Relay profile.

Command Mode

Frame Relay profile configuration

Syntax Description

value	Transmit queue size in number of packets. The range of values is 1 to 63; the default is 50.

Default

The transmit queue size is 50.

Usage Guidelines

Use the **buffers transmit** command to controls the size of the transmit queue for any circuit referencing this Frame Relay profile.

Use the **default** form of this command to reset the number of transmit buffers back to the default value.

Examples

The following example configures a transmit queue size of `30` for the Frame Relay profile named `frame20`:

```
[local]RedBack(config)#frame-relay profile frame20
[local]RedBack(config-frpro)#buffers transmit 30
```

Related Commands

buffers—port configuration mode
show frame-relay profile

bulkstats schema

bulkstats schema *schema-name* **format** *format-string* [*AOS-variable* [*AOS-variable* …]]

no bulkstats schema *schema-name*

Purpose

Defines the schema for the contents of the bulkstats collection file for any circuit referencing the Frame Relay profile.

Command Mode

Frame Relay profile configuration

Syntax Description

schema-name	Name of the schema. Cannot be longer than 19 characters in length.
format *format-string*	String used to format the output of the schema. The format string can contain anything or nothing as a label for an Access Operating System (AOS) variable. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. Table 18-1 describes the supported special-character sequences.
AOS-variable	Optional. Variables for which data is collected. An AOS variable replaces its associated *format-string* definition. Separate the variables with a space. Table 18-2 lists all available AOS variables in Frame Relay profile configuration mode.

Table 18-1 C Programming Language printf() Syntax

Syntax	Description
%s	A character string
%d	An integer in decimal (base 10)
%u	An unsigned integer in decimal (base 10)
%x	An integer in hexadecimal format (base 16)
%%	Gets replaced by a single % character in the output
\n	UNIX newline character

Table 18-2 AOS Variables

AOS Variable	Type	Description
slot	Integer	Slot number in the SMS
port	Integer	Port number on the I/O module
description	String	Description of port
sysuptime	Integer	System uptime in seconds
inoctets	Integer	Number of octets received on this circuit
outoctets	Integer	Number of octets sent from this circuit
inpackets	Integer	Number of packets received on this circuit
outpackets	Integer	Number of packets sent on this circuit
mcast_inoctets	Integer	Number of multicast octets received on this circuit
mcast_outoctets	Integer	Number of multicast octets sent on this circuit
mcast_inpackets	Integer	Number of multicast packets received on this circuit
mcast_outpackets	Integer	Number of multicast packets sent on this circuit

Default

No schema is defined for the profile.

Usage Guidelines

Use the **bulkstats schema** command to define the schema for the contents of the bulkstats collection file for any circuit referencing a Frame Relay profile. You can configure multiple schemas, each gathering a different type and format of data. However, you should restrict the use of multiple schemas to global data collection and create only one schema per port, circuit, or profile. Otherwise, you can apply a profile with several schemas to a large number of circuits, slowing down the Subscriber Management System (SMS) processor function.

If you want to generate multiple collections of bulk statistics for a single port, circuit, or profile, create one schema designed to record separate groups of distinct data (subschemas) using the **\n** character sequence after each subset entry to create a new starting line.

When multiple schemas are defined in a configuration mode, each of the schemas is used to create a text record that is appended to the bulkstats collection file each sample period. Every line created always has the same schema name as the first field and has a newline appended as a record separator.

Use the **no** form of this command to remove the named bulkstats schema from the Frame Relay profile.

Examples

The following example defines a bulkstats schema for a Frame Relay profile that includes the system uptime, slot number, port number, number of octets received, and number of octets transmitted:

```
[local]RedBack(config-frpro)#bulkstats schema example format "frm:%s, slot:%u, port:%u,
inoct:%u, outoct:%u" sysuptime slot port inoctets outoctets
```

The previous example creates a line in the collection file that looks like the following:

```
host1: frm:348765, slot:3, port:1, inoct:234975, outoct:165444
```

Related Commands

bulkstats collection
bulkstats schema—HDLC channel configuration mode
bulkstats schema—port configuration mode

clear lmi-counters

clear lmi-counters *slot/port* [**all** | **hdlc-channel** *chan-name*] [**-noconfirm**]

Purpose

Clears Frame Relay Local Management Interface (LMI) statistics and error counters.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot and port number of the configured Frame Relay port.
all	Specifies that all error and statistics information for all HDLC channels on a channelized DS-3 port is cleared. Available only for channelized DS-3 ports.
hdlc-channel *chan-name*	Name of an HDLC channel for which the LMI counters are cleared. Available only for channelized DS-3 ports.
-noconfirm	Optional. Specifies that the command is executed without a confirmation prompt.

Default

Clears all LMI counters on the specified port.

Usage Guidelines

Use the **clear lmi-counters** command to clear Frame Relay Local Management Interface (LMI) statistics and error counters. This command only affects the counters available to the command line. Corresponding Simple Network Management Protocol (SNMP) counters are not cleared.

For channelized DS-3 ports, you must specify either the **all** keyword or the **hdlc-channel** *chan-name* construct. For all other ports, you can not specify these options.

Examples

The following example clears LMI counters on a Frame Relay port:

```
[local]RedBack#clear lmi-counters 4/0 -noconfirm
```

The next example clears LMI counters for all channels on a channelized DS-3 port:

```
[local]RedBack#clear lmi-counters 5/0 all -noconfirm
```

Related Commands

clear port counters
show frame-relay lmi-errors
show frame-relay lmi-stats

counters

counters [**l2** | **multicast**]

{**no** | **default**} **counters**

Purpose

Enables statistics to be collected by the system for any circuit referencing this Frame Relay profile.

Command Mode

Frame Relay profile configuration

Syntax Description

l2	Optional. Enables statistics collection for only layer 2 packets.
multicast	Optional. Enables statistics collection for only multicast (layer 3) traffic.

Default

Statistics are not collected by the system.

Usage Guidelines

Use the **counters** command to enable the collection of statistics by the system for any circuit referencing this Frame Relay profile. To enable statistics collection for both layer 2 and layer 3 packets, do not specify any optional keywords with the command. To enable statistics collection for only layer 2 packets, use the **counters l2** command. To enable statistics collection for only multicast traffic, use the **counters multicast** command.

Statistics are not collected by default because of the potentially large amount of memory needed. If memory usage is a problem, disabling any unnecessary multicast counters on circuits can substantially help.

Note For the **aaa accounting subscriber radius** command, accounting packets only include packet and byte counts for a given circuit if the **counters** command is enabled in the Frame Relay profile referenced by that circuit.

To obtain multicast statistics, Internet Group Management Protocol (IGMP) proxy must be enabled on the interface and context to which the circuit is bound. See the **ip multicast-routing** (context configuration mode), **ip igmp** (interface configuration mode), **ip multicast-routing** and **ip multicast receive** (subscriber configuration mode), and **router-igmp-interface** (IGMP proxy router configuration mode) commands.

Use the **no** or **default** form of this command to disable statistics collection.

Examples

The following example configures a Frame Relay profile named `frame20` to enable per-permanent virtual circuit (PVC) statistics collection for both layer 2 packets and multicast (layer 3) traffic on all Frame Relay PVCs that are configured to reference that profile:

```
[local]RedBack(config)#frame-relay profile frame20
[local]RedBack(config-frpro)#counters
```

Related Commands

aaa accounting
ip igmp
ip multicast receive
ip multicast-routing—context configuration mode
ip multicast-routing—subscriber configuration mode
router-igmp-interface
show frame-relay counters
show frame-relay multicast
show frame-relay profile

debug frame-relay lmi

debug frame-relay lmi [*slot/port*]

no debug frame-relay lmi [*slot/port*]

Purpose

Enables the logging of Local Management Interface (LMI) packet exchanges with the service provider.

Command Mode

administrator exec

Syntax Description

slot/port	Optional. Backplane slot and port number.

Default

Debugging is disabled. The default, if debugging is enabled without the optional *slot/port* argument, is to log LMI messages for all ports.

Usage Guidelines

Use the **debug frame-relay lmi** command to enable the logging of LMI packet exchanges with the service provider. As a default, the debug output is sent to the log. If you want to have debug output sent to the console, you must enter the **logging console** global configuration command. If you are connected via Telnet and you want the debug output to be displayed on your screen, you must enter the **terminal monitor** command.

Caution Debugging can severely affect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to disable logging of LMI packet exchanges.

Examples

The following example shows sample output when LMI debugging is enabled and two ports are looped together, with port `3/0` being the Data Communications Equipment (DCE) LMI interface, and port `3/1` the Data Terminal Equipment (DTE) interface:

```
[local]RedBack#debug frame-relay lmi

17:17:57 8Jun1998: %FR-6-LMI_MSG: Port 3/1(out): StEnq,  myseq 14
17:17:57 8Jun1998: %FR-6-LMI_RTIE: RT IE 0x51, length 1, type 1 (link-integrity)
17:17:57 8Jun1998: %FR-6-LMI_KAIE: KA IE 0x53, length 2, yourseq 5, myseq 14
17:17:57 8Jun1998: %FR-6-LMIENCAP: FR encap = 0x00010308, size = 13 :
  0x00 75 51 01 01 53 02 0e 05
17:17:57 8Jun1998: %FR-6-LMI_MSG: Port 3/0(in): StEnq,  myseq 5
17:17:57 8Jun1998: %FR-6-LMI_RTIE: RT IE 0x51, length 1, type 1 (link-integrity)
17:17:57 8Jun1998: %FR-6-LMI_KAIE: KA IE 0x53, length 2, yourseq 14, myseq 5
17:17:57 8Jun1998: %FR-6-LMIENCAP: FR encap = 0x00010308, size = 13 :
  0x00 75 51 01 01 53 02 0e 05
17:17:57 8Jun1998: %FR-6-LMI_MSG: Port 3/0(out): Status, myseq 6
17:17:57 8Jun1998: %FR-6-LMI_RTIE: RT IE 0x51, length 1, type 1 (link-integrity)
17:17:57 8Jun1998: %FR-6-LMI_MSG: KA IE 0x53, length 2, yourseq 14, myseq 6, DCE  UP
17:17:57 8Jun1998: %FR-6-LMI_MSG: Port 3/1(in): Status, myseq 14
17:17:57 8Jun1998: %FR-6-LMI_RTIE: RT IE 0x51, length 1, type 1 (link-integrity)
17:17:57 8Jun1998: %FR-6-LMI_MSG: KA IE 0x53, length 2, yourseq 6, myseq 14, DTE  UP
```

Related Commands

debug frame-relay packet
logging console
show cm stats
show frame-relay lmi-config
terminal monitor

debug frame-relay packet

debug frame-relay packet

no debug frame-relay packet

Purpose

Enables debugging of all non-Local Management Interface (LMI) Frame Relay packets.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug frame-relay packet** command to enable debugging of all non-LMI Frame Relay packets. As a default, the debug output is sent to the log. If you want to have debug output sent to the console, you must enter the **logging console** global configuration command. If you are connected via Telnet and you want the debug output to be displayed on your screen, you must enter the **terminal monitor** command.

Caution Debugging can severely affect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to turn off debugging of non-LMI Frame Relay packets.

Examples

The following example shows sample debug output after sending a single ping packet on data-link connection identifier (DLCI) 16, using RFC 1490 routed encapsulation:

```
[local]RedBack#debug frame-relay packet

17:26:53 8Jun1998: %FR-6-PKT_ROUTED: Port 3/0(o): dlci 16(0x0401),
     routed, NLPID 0xcc03(IP), size 124
17:26:53 8Jun1998: %FR-6-PKT_ROUTED: Port 3/0(i): dlci 16(0x0401),
```

```
routed, NLPID 0xcc03(IP), size 124
```

Related Commands

debug frame-relay lmi
logging console
show cm stats
terminal monitor

frame-relay auto-detect

frame-relay auto-detect

no frame-relay auto-detect

default frame-relay auto-detect

Purpose

Configures the Local Management Interface (LMI) to automatically determine which data-link connection identifier (DLCI) to use for LMI packets.

Command Mode

port configuration

Syntax Description

This command has no keywords or arguments.

Default

Auto-detection is enabled.

Usage Guidelines

Use the **frame-relay auto-detect** command to configure the LMI to automatically determine which DLCI to use for LMI packets. Auto-detect tells the system to look at the first LMI message received from the remote end, determine from the message the LMI type of the remote end, and reconfigure the LMI type at the local end to match.

The original “group of 4” LMI uses DLCI number 1023 as the PVC number, while both the ANSI and ITU LMI use DLCI number 0. If the LMI type is not set to Group-of-Four (using the **frame-relay lmi-type** command) and the local Frame Relay interface type is Data Communications Equipment (DCE), this command allows the software to detect which LMI type is being used by the remote end and use that same LMI type at the local end.

By default, auto-detect is enabled. Also, the default LMI type is ANSI. However, the default interface type is Data Terminal Equipment (DTE), so auto-detect does not normally operate. However, if you configure the interface type to be DCE, then auto-detect would take effect (unless previously disabled on the command line).

Use the **no** form of this command to disable auto-detection of the DLCI.

Use **default** form of this command to enable auto-detection of the DLCI.

Examples

The following example disables automatic detection of the DLCI to use for LMI on DS-3 port 7/0:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#no frame-relay auto-detect
```

Related Commands

frame-relay intf-type
frame-relay lmi-type

frame-relay intf-type

frame-relay intf-type {**dce** | **dte** | **nni**}

default frame-relay intf-type

Purpose

Configures the Frame Relay interface as Data Communications Equipment (DCE), Data Terminal Equipment (DTE), or Network to Network Interface (NNI).

Command Mode

port configuration

Syntax Description

dce	Specifies that the port functions as a switch connected to a communications server.
dte	Specifies that the port is connected to a Frame Relay network.
nni	Specifies that the port functions as a switch connected to a switch.

Default

Frame Relay interfaces are set to DTE.

Usage Guidelines

Use the **frame-relay intf-type** command to configure the interface type for the Frame Relay port.

If you configure the interface type as DCE and the Local Management Interface (LMI) is not disabled, LMI Status Enquiries are expected to be received by the port, and Status messages are sent as a response.

If you configure the interface type as DTE and LMI is not disabled, LMI Status Enquiries are sent by the port, and Status messages are expected to be received.

If you configure the interface type as NNI and LMI is not disabled, LMI Status Enquiries are both sent and received by the port, and Status messages are also both sent and received.

This command is completely independent of the **clock-source** command for clear-channel DS-3 cards, and the **hardware-interface** command for High-Speed Serial Interface (HSSI) cards. For example, you can set the LMI interface to DCE on a HSSI port that you have configured with a DTE hardware interface.

Use the **default** form of this command to return the Frame Relay interface setting to its default of DTE.

Examples

The following example configures a clear-channel DS-3 port in slot 7 as an NNI interface:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay intf-type nni
```

Related Commands

clock-source
frame-relay lmi-type
hardware-interface

frame-relay keepalive

frame-relay keepalive *seconds*

no frame-relay keepalive

default frame-relay keepalive

Purpose

Modifies the interval between transmissions of keepalive messages by a Frame Relay Data Terminal Equipment (DTE) or network-to-network interface (NNI).

Command Mode

port configuration

Syntax Description

seconds	Number of seconds between keepalive messages. The range of values is 0 to 60; the default value is 10.

Default

Keepalives are enabled, with a 10-second interval between transmissions.

Usage Guidelines

Use the **frame-relay keepalive** command to configure the interval between transmissions of keepalive messages. You can only use this command when you have configured the Frame Relay interface type as DTE or NNI (using the **frame-relay intf-type** port configuration command).

Use the **no** form of this command (or the **frame-relay keepalive 0** command) to turn off transmission of keepalives completely. This allows connections to time out and terminate during periods of inactivity.

Use the **default** form of this command to set the keepalive transmission interval to the default of 10 seconds.

Examples

The following example sets the keepalive interval on a specific port to `20` seconds:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay keepalive 20
```

Related Commands

frame-relay intf-type

frame-relay lmi-n391dte

frame-relay lmi-n391dte *exchanges*

no frame-relay lmi-n391dte

d**efault frame-relay lmi-n391dte**

Purpose

Specifies the number of keepalive messages to be sent before a request for a full status message is sent.

Command Mode

port configuration

Syntax Description

exchanges	Number of keepalive exchanges to be done before requesting a full status message. The range of values is 0 to 255; the default value is 6.

Default

The number of keepalive exchanges is 6.

Usage Guidelines

Use the **frame-relay lmi-n391dte** command to configure the number of keepalive messages to be sent before a request for a full status message is sent. You can only use this command when you have configured the Frame Relay interface type as DTE or NNI (using the **frame-relay intf-type** port configuration command).

Use the **no** form of this command to set the number of keepalive exchanges to 0. In this case, all keepalive messages requests a full status message.

Use the **default** form of the command to return the setting to the default value of 6.

Examples

The following example sets the number of keepalive exchanges before a full status message to `10`:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay lmi-n391dte 10
```

Related Commands

frame-relay intf-type

frame-relay lmi-n392dce

frame-relay lmi-n392dce *threshold*

no frame-relay lmi-n392dce

default frame-relay lmi-n392dce

Purpose

Sets the error threshold before the Local Management Interface (LMI) is considered to have failed on a Data Communications Equipment (DCE) or network-to-network (NNI) interface.

Command Mode

port configuration

Syntax Description

threshold	Error threshold in number of errors. The range of values is 0 to 10; the default value is 3.

Default

The threshold is 3.

Usage Guidelines

Use the **frame-relay lmi-n392dce** command to set the error threshold before LMI is considered to have failed on a DCE or NNI interface. You can only use this command when you have configured the Frame Relay interface type as DCE or NNI (using the **frame-relay intf-type** port configuration command).

The error threshold should never be greater than the monitored event count (configured with the **frame-relay lmi-n393dce** port configuration command) because when the error threshold meets or exceeds the monitored event count, the LMI is considered to have failed.

Use the **no** form of this command to set the threshold value to 0.

Use the **default** form of this command to set the error threshold to the default value of 3.

Examples

The following example sets the error threshold to `5` on a `DCE` interface:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay intf-type dce
[local]RedBack(config-port)#frame-relay lmi-n392dce 5
```

Related Commands

frame-relay intf-type
frame-relay lmi-n392dte
frame-relay lmi-n393dce

frame-relay lmi-n392dte

frame-relay lmi-n392dte *threshold*

no frame-relay lmi-n392dte

default frame-relay lmi-n392dte

Purpose

Sets the error threshold before the Local Management Interface (LMI) considered to have failed on a Data Terminal Equipment (DTE) or network-to-network interface (NNI).

Command Mode

port configuration

Syntax Description

threshold	Error threshold in number of errors. The range of values is 0 to 10; the default value is 3.

Default

The threshold is 3.

Usage Guidelines

Use the **frame-relay lmi-n392dte** command to set the error threshold before LMI is considered to have failed on a DTE or NNI interface. You can only use this command when you have configured the Frame Relay interface as either DTE or NNI (using the **frame-relay intf-type** port configuration command).

The error threshold should never be greater than the monitored event count (configured with the **frame-relay lmi-n393dte** command) because when the error threshold meets or exceeds the monitored event count, the LMI is considered to have failed.

Use the **no** form of this command to set the threshold value to 0.

Use the **default** form of this command to set the error threshold to the default value of 3.

Examples

The following example sets the error threshold to `5` on a `DTE` interface:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay intf-type dte
[local]RedBack(config-port)#frame-relay lmi-n392dte 5
```

Related Commands

frame-relay intf-type
frame-relay lmi-n392dce
frame-relay lmi-n393dte

frame-relay lmi-n393dce

frame-relay lmi-n393dce *event-count*

no frame-relay lmi-n393dce

default frame-relay lmi-n393dce

Purpose

Sets the monitored event count on a Data Communications Equipment (DCE) or network-to-network (NNI) interface.

Command Mode

port configuration

Syntax Description

event-count	Number of events (receipts of messages across the interface) to be included in the monitored event count. The range of values is 0 to 10; the default is 4.

Default

The monitored event count is enabled and set to 4.

Usage Guidelines

Use the **frame-relay lmi-n393dce** command to set the monitored event count on a DCE or NNI interface. You can only use this command if you have configured the Frame Relay interface type as DCE or NNI.

The event count should never be less than the error threshold count (configured by the **frame-relay lmi-n392dce** command), because when the error threshold meets or exceeds the monitored event count, the Local Management Interface (LMI) is considered to have failed.

Use the **no** form of this command to set the monitored event count value to 0.

Use the **default** form of this command to set the monitored event count to the default value of 4.

Examples

The following example sets the monitored event count to 5 on a DCE interface:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay intf-type dce
[local]RedBack(config-port)#frame-relay lmi-n393dce 5
```

Related Commands

frame-relay intf-type
frame-relay lmi-n392dce
frame-relay lmi-n393dte

frame-relay lmi-n393dte

frame-relay lmi-n393dte *event-count*

no frame-relay lmi-n393dte

default frame-relay lmi-n393dte

Purpose

Sets the monitored event count on a Data Terminal Equipment (DTE) or network-to-network interface (NNI).

Command Mode

port configuration

Syntax Description

event-count	Number of events (receipts of messages across the interface) to be included in the monitored event count. The range of values is 0 to 10; the default is 4.

Default

The monitored event count is enabled and set to 4.

Usage Guidelines

Use the **frame-relay lmi-n393dte** command to set the monitored event count on a DTE or NNI interface. You can only use this command when you have configured the Frame Relay interface type as DTE or NNI (using the **frame-relay intf-type** command).

The event count should never be less than the error threshold count (configured using the **frame-relay lmi-n392dte** command) because when the error threshold meets or exceeds the monitored event count, the Local Management Interface (LMI) is considered to have failed.

Use the **no** form of this command to set the monitored event count value to 0.

Use the **default** form of this command to set the monitored event count to the default value of 4.

Examples

The following example sets the monitored event count to `5` on a `DTE` interface:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay intf-type dte
[local]RedBack(config-port)#frame-relay lmi-n393dte 5
```

Related Commands

frame-relay intf-type
frame-relay lmi-n392dte
frame-relay lmi-n393dce

frame-relay lmi-t392dce

frame-relay lmi-t392dce *seconds*

no frame-relay lmi-t392dce

default frame-relay lmi-t392dce

Purpose

Sets the polling verification timer on a Data Communications Equipment (DCE) or network-to-network (NNI) interface.

Command Mode

port configuration

Syntax Description

seconds	Number of seconds after which an error is counted if a message has not been received. The range of values is 5 to 30; the default is 15.

Default

The polling verification timer is enabled and set to 15 seconds.

Usage Guidelines

Use the **frame-relay lmi-t392dce** command to set the polling verification timer when the Frame Relay interface type is configured as DCE or NNI. The value should be greater than the keepalive timer that is set by the remote end.

The polling verification timer starts each time a keepalive message is received from the remote end. If no keepalive message is received before the timer expires, an error is counted. If the number of errors exceeds the error threshold, the LMI is declared down.

Use the **no** form of this command to turn off the timer.

Use the **default** form of this command to set the polling verification timer to the default value of 15 seconds.

Examples

The following example sets the polling verification timer to 5 seconds on a DCE interface:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay intf-type dce
[local]RedBack(config-port)#frame-relay lmi-t392dce 5
```

Related Commands

frame-relay intf-type
frame-relay keepalive
frame-relay lmi-n392dce

frame-relay lmi-type

frame-relay lmi-type {**ansi** | **group-of-4** | **itu**}

no frame-relay lmi-type

default frame-relay lmi-type

Purpose

Configures the Frame Relay Local Management Interface (LMI) type.

Command Mode

port configuration

Syntax Description

ansi	Specifies the LMI type for Annex D as defined by ANSI standard T1.617.
group-of-4	Specifies the original LMI as defined by Cisco, DEC, Northern Telecom, and StrataCom.
itu	Specifies the LMI type for ITU-T Q933 Annex A (formerly labeled as CCITT).

Default

The LMI type is ANSI.

Usage Guidelines

Use the **frame-relay lmi-type** command to configure the LMI type for the Frame Relay interface.

Note Packet over Synchronous Optical Network (POS) ports only support the ANSI LMI type.

Use the **no** form of this command to disable the LMI interface. Setting the **frame-relay keepalive** timer to zero has the same effect.

Use the **default** form of this command to set the LMI type to the default of ANSI.

Examples

The following example configures the specified port to use an LMI type of ITU-T Q933 Annex A:

```
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay lmi-type itu
```

Related Commands

clock-source
frame-relay intf-type
frame-relay keepalive
hardware-interface

frame-relay profile

frame-relay profile *prof-name*

no frame-relay profile *prof-name*

Purpose

Creates a Frame Relay profile with the given name (if it does not already exist) and enters Frame Relay profile configuration mode.

Command Mode

global configuration

Syntax Description

prof-name	Alphanumeric string name given to the particular profile.

Default

No Frame Relay profiles are defined.

Usage Guidelines

Use the **frame-relay profile** command to create a Frame Relay profile and enter Frame Relay profile configuration mode. You must create a Frame Relay profile before you can create a Frame Relay permanent virtual circuit (PVC) that references it.

Use the **no** form of this command to delete a Frame Relay profile. You cannot delete a profile if it is being referenced by any Frame Relay PVC.

Examples

The following command creates a Frame Relay profile named `frame20` and enters Frame Relay profile configuration mode.

```
[local]RedBack(config)#frame-relay profile frame20
[local]RedBack(config-frpro)#
```

Related Commands

frame-relay pvc
show frame-relay profile

frame-relay pvc

frame-relay pvc *dlci* [**through** *end-dlci*] **profile** *prof-name* **encapsulation** {**auto1490** | **bridge1490** | **route 1490** | **dot1q** | **l2tp** | **multi** | **ppp** [**auto** | **over-ethernet**]}

no frame-relay pvc *dlci* [**through** *end-dlci*]

Purpose

Configures one or a series of Frame Relay permanent virtual circuits (PVCs) on a given Frame Relay port, and enters circuit configuration mode.

Command Mode

port configuration

Syntax Description

dlci	Data-link connection identifier (DLCI) of the individual circuit or the first DLCI in a range of circuits to be configured. The range of values is 16 to 991.
through *end-dlci*	Optional. DLCI of the last circuit in a range of circuits to be configured.
profile *prof-name*	Existing Frame Relay profile to use for the PVC.
encapsulation	Specifies the encapsulation type for the PVC (from the keywords that follow).
auto1490	Enables auto detection between RFC 1490 bridged and routed encapsulations.
bridge1490	Specifies RFC 1490 bridged encapsulation.
route1490	Specifies RFC 1490 routed encapsulation.
dot1q	Specifies that the PVC carries 802.1Q traffic.
l2tp	Specifies that the PVC carries a Layer 2 Tunnel Protocol (L2TP) tunnel.
multi	Specifies that the circuit contains both RFC 1490 bridged and PPP over Ethernet (PPPoE) encapsulations.
ppp	Specifies Point-to-Point Protocol (PPP) encapsulation. When you use this keyword without a qualifying keyword, the default encapsulation is standard PPP over Frame Relay.
auto	Optional. Enables auto-detection among the PPP encapsulation types.
over-ethernet	Optional. Specifies PPPoE encapsulation.

Default

No PVCs are defined.

Usage Guidelines

Use the **frame-relay pvc** command to create or configure a Frame Relay PVC or a range or PVCs with similar characteristics. You can use this command to modify a subset of PVCs that have been defined with the **frame-relay pvc explicit** and **frame-relay pvc on-demand** commands. The Frame Relay profile you specify must exist prior to using this command.

Use the **through** keyword to provision groups of similar PVCs on an Frame Relay port. The following guidelines apply when you use the **through** keyword:

- Any Frame Relay PVCs in the specified range that do not already exist are created with the specified profile and encapsulation.
- Any Frame Relay PVCs in the specified range that do exist (including those defined with the **frame-relay pvc explicit** and **frame-relay pvc on-demand** commands) are modified to use the specified profile and encapsulation.
- The **bind subscriber** and **ip host** commands cannot be used in conjunction with the **frame-relay pvc through** command. You can create a PVC range, then subsequently modify individual PVCs if use of these commands is required.
- When you use the **no** form of this command in conjunction with the **through** keyword, all Frame Relay PVCs in the range are deleted, regardless of whether those PVCs have the same profile and encapsulation. You can delete a subset of PVCs.

Note When you use the **through** keyword with this command, the Access Operating System (AOS) generates a single command in the configuration for each PVC in the specified range. To avoid a large configuration file, use the **frame-relay pvc explicit** command to configure explicit PVC ranges.

When you specify the **dot1q** keyword for the encapsulation, you can create 802.1Q PVCs on the circuit.

Two forms of auto detection are possible with this command. The **auto1490** keyword enables auto detection between RFC 1490 bridged and routed encapsulations, and the **ppp auto** keyword enables auto detection among the various PPP encapsulations.

When you select the **auto1490** keyword, the circuit mode commands that become visible are the union of those available for the **bridge1490** and **route1490** keywords. The Access Operating System (AOS) handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **ip host** *ip-address* [*mac-address*] command accepts both forms (with or without the *mac-address* argument) for the **bind interface** command, and puts a message into the system log if the wrong type of command is entered for the type of encapsulation eventually detected.

When you select the **ppp auto** keywords, the circuit mode commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. AOS handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **bind authentication** command accepts the **max-sessions** keyword, which is ignored (effectively set to 1) if the encapsulation is not PPPoE.

Use the **no** form of this command to delete a previously configured PVC or a range of PVCs. The **no** form of this command does not affect PVCs that have been defined with the **frame-relay pvc explicit** or **frame-relay pvc on-demand** command.

Examples

The following example configures a PVC with DLCI `30` to use the `frame20` profile and RFC 1490 bridged encapsulation:

```
[local]RedBack(config)#frame-relay profile frame20
[local]RedBack(config-frpro)#counters
[local]RedBack(config-frpro)#exit
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay pvc 30 profile frame20 encapsulation bridge1490
[local]RedBack(config-pvc)#
```

The next example configures a PVC to auto-detect between RFC 1490 bridged and routed encapsulations:

```
[local]RedBack(config-port)#frame-relay pvc 30 profile ubr encapsulation auto1490
[local]RedBack(config-pvc)#bind subscriber fred@local
```

The next example configures a series of PVCs, all with the same profile and encapsulation:

```
[local]RedBack(config)#frame-relay profile frame20
[local]RedBack(config-frpro)#counters
[local]RedBack(config-frpro)#exit
[local]RedBack(config)#port ds3 7/0
[local]RedBack(config-port)#frame-relay pvc 30 through 100 profile frame20
encapsulation ppp
[local]RedBack(config-pvc)#bind authentication pap
```

The next example configures a series of PVCs configured to auto-detect between RFC 1490 bridged and routed encapsulations:

```
[local]RedBack(config-port)#frame-relay pvc 30 through 100 profile frame20
encapsulation auto1490
[local]RedBack(config-pvc)#bind authentication pap
```

Related Commands

frame-relay profile
frame-relay pvc explicit
frame-relay pvc on-demand
show frame-relay profile
show frame-relay pvc

frame-relay pvc explicit

frame-relay pvc explicit *start-dlci* **through** *end-dlci* **profile** *prof-name* **encapsulation** {**auto1490** | **bridge1490** | **route1490** | **multi** | **ppp** [**auto** | **over-ethernet**]}

no frame-relay pvc explicit *start-dlci* **through** *end-dlci*

Purpose

Sets the default profile and encapsulation for Frame Relay circuits on a Frame Relay port and enters circuit configuration mode for an explicit range of Frame Relay permanent virtual circuits (PVCs).

Command Mode

port configuration

Syntax Description

start-dlci	Data-link connection identifier (DLCI) of the first circuit in the range. The range of values is 16 to 991.
through *end-dlci*	DLCI of the last circuit in the range. The range of values is 16 to 991.
profile *prof-name*	Name of the profile to be used as the default.
encapsulation	Specifies the encapsulation type (from the following keywords).
auto1490	Enables auto-detection with regard to choosing between RFC 1490 bridged and routed encapsulations.
bridge1490	Specifies RFC 1490 bridged encapsulation.
route1490	Specifies RFC 1490 routed encapsulation.
multi	Specifies that the circuit contains both RFC 1490 bridged and PPPoE encapsulations.
ppp	Specifies Point-to-Point Protocol (PPP) encapsulation. When you use this keyword without a qualifying keyword, the default encapsulation is standard PPP over Frame Relay.
auto	Optional. Enables auto-detection with regard to the PPP encapsulation type.
over-ethernet	Optional. Selects PPP over Ethernet (PPPoE) encapsulation.

Default

None

Usage Guidelines

Use the **frame-relay pvc explicit** command to create a range of Frame Relay PVCs that share the same profile and encapsulation. This command generates a single command in the configuration file. You can use the **frame-relay pvc** command to overwrite one or more of the PVCs in a range defined by the **frame-relay pvc explicit** command.

The following guidelines apply to this command:

- You cannot overwrite a PVC range that was previously configured with the **frame-relay pvc explicit** or **frame-relay pvc on-demand** commands, except if the new range completely encompasses that previous range.
- If you use this command to overwrite a PVC range that was previously defined with the **frame-relay pvc on-demand** command, all active circuits are cleared.
- You can use the **frame-relay pvc** command to overwrite one or more PVCs defined by the **frame-relay pvc explicit** command. If you subsequently use the **no frame-relay pvc** command to delete such a PVC, the PVC reverts to the **frame-relay pvc explicit** definition.
- You cannot use the **no frame-relay pvc** command to remove PVCs from an explicit range.
- You cannot use the **bind subscriber** and **ip host** commands in conjunction with this command. You can create a PVC range, then subsequently modify individual PVCs if use of these commands is required.

Two forms of auto detection are possible with this command. The **auto1490** keyword enables auto detection between RFC 1490 bridged and routed encapsulations, and the **ppp auto** keywords enable auto detection among the various PPP encapsulations.

When you select the **auto1490** keyword, the circuit mode commands that become visible are the union of those available for the **bridge1490** and **route1490** keywords. The Access Operating System (AOS) handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **ip host** *ip-address* [*mac-address*] command accepts both forms (with or without the *mac-address* argument) for the **bind interface** command, and puts a message into the system log if the wrong type of command is entered for the type of encapsulation eventually detected.

When you select the **ppp auto** keywords, the circuit mode commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. AOS handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **bind authentication** command accepts the **max-sessions** keyword, which is ignored (effectively set to 1) if the encapsulation is not PPPoE.

Use the **no** form of this command to remove the specified range of circuits. You must specify the same circuit range as specified in the **frame-relay pvc explicit** command.

Examples

The following example creates an explicit range of `100` Frame Relay PVCs that use the profile named `adam` and `auto1490` encapsulation:

```
[local]RedBack(config-port)#frame-relay pvc explicit 100 through 199 profile adam
encapsulation auto1490
[local]RedBack(config-pvc)#bind authentication chap pap
```

Related Commands

frame-relay profile
frame-relay pvc
frame-relay pvc on-demand
show frame-relay profile
show frame-relay pvc

frame-relay pvc on-demand

frame-relay pvc on-demand *start-dlci* **through** *end-dlci* {**profile** *prof-name* **encapsulation** {**auto1490** | **bridge1490** | **route1490** | **multi** | **ppp** [**auto** | **over-ethernet**]} | **aaa context** *ctx-name* [**prefix-string** *text*]}

no frame-relay pvc on-demand *start-dlci* **through** *end-dlci*

Purpose

Creates a range of Frame Relay permanent virtual circuits (PVCs) that are configured automatically as activity is detected on the circuits.

Command Mode

port configuration

Syntax Description

start-dlci	Data-link connection identifier (DLCI) of the first circuit in the range. The range of values is 16 to 991.
through *end-dlci*	DLCI of the last circuit in the range. The range of values is 16 to 991.
profile *prof-name*	Name of the profile to be used as the default.
encapsulation	Specifies the encapsulation type (from the following keywords).
auto1490	Enables auto-detection with regard to choosing between RFC 1490 bridged and routed encapsulations.
bridge1490	Specifies RFC 1490 bridged encapsulation.
route1490	Specifies RFC 1490 routed encapsulation.
multi	Specifies that the circuit contains both RFC 1490 bridged and PPPoE encapsulations.
ppp	Specifies Point-to-Point Protocol (PPP) encapsulation. When you use this keyword without a qualifying keyword, the default encapsulation is standard PPP over Frame Relay.
auto	Optional. Enables auto-detection with regard to the Point-to-Point Protocol (PPP) encapsulation type.
over-ethernet	Optional. Selects PPP over Ethernet (PPPoE) encapsulation.
aaa	Specifies that the circuits are to be created using Remote Authentication Dial-in User Service (RADIUS).
context *ctx-name*	Name of the context in which the RADIUS servers configured are to be used for authentication, authorization, and accounting (AAA) configuration.

prefix-string *text*	String to be used as a prefix in constructing the User-Name attribute. Must not contain spaces, periods, underscores, forward slashes, or backward slashes.

Default

None

Usage Guidelines

Use the **frame-relay pvc on-demand** command to create a range of PVCs that are configured automatically as activity is detected on the circuits.

The following guidelines apply to this command:

- You cannot use this command to overwrite a PVC range that was previously configured with the **frame-relay pvc explicit** or **frame-relay pvc on-demand** command, except if the new range completely encompasses that previous range.
- If you use this command to overwrite a PVC range that was previously defined with the **frame-relay pvc explicit** command, the circuits are not cleared. You must use the **clear circuit** command to manually clear these circuits.
- You can use the **frame-relay pvc** command to overwrite one or more PVCs defined by this command. If you subsequently delete such a PVC with the **no frame-relay pvc** command, the PVC reverts to the **frame-relay pvc on-demand** definition.
- You cannot use the **no frame-relay pvc** command to remove PVCs from an on-demand range.
- You cannot use the **bind subscriber** and **ip host** commands in conjunction with this command. You can create a PVC range, then subsequently modify individual PVCs if use of these commands is required.

Two forms of auto detection are possible with this command. The **auto1490** keyword enables auto detection between RFC 1490 bridged and routed encapsulations, and the **ppp auto** keywords enable auto detection among the various PPP encapsulations.

When you specify the **auto1490** keyword, the circuit mode commands that become visible are the union of those available for the **bridge1490** and **route1490** keywords. The Access Operating System (AOS) handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **ip host** *ip-address* [*mac-address*] command accepts both forms (with or without the *mac-address* argument) for the **bind interface** command, and puts a message into the system log if the wrong type of command is entered for the type of encapsulation eventually detected.

When you specify the **ppp auto** keyword, the circuit mode commands that become visible are a union of those available for PPPoE and the non-PPPoE encapsulations. AOS handles the information entered in circuit mode commands appropriately, once the encapsulation is auto-detected. Specifically, the **bind authentication** command accepts a **max-sessions** specification, which is ignored (effectively set to 1) if the encapsulation is not PPPoE.

When you create a range of on-demand Frame Relay PVCs, you can use the **profile** and **encapsulation** keywords to specify the profile and encapsulation type explicitly. Or, you can use the **aaa** keyword to configure AOS to use RADIUS to configure the profile, encapsulation, and binding of the circuits in the range. If you use the **aaa** keyword, you must specify the context that the RADIUS servers are defined in with the **context** *ctx-name* construct.

You can also define a prefix-string that is used to construct the User-Name attribute. By default, the RADIUS User-Name is in the form *hostname.port.slot.*[*hdlc-channel*].*dlci*. The *hdlc-channel* argument is included for channelized DS-3 ports only. If you define a prefix string, the RADIUS User-Name attribute is in the form: *prefix-string.*[*hdlc-channel*].*dlci*.

When you use the **aaa** keyword, this command does not enter circuit configuration mode.

Use the **no** form of this command to remove the specified range of circuits. You must specify the same circuit range as specified in the **frame-relay pvc on-demand** command.

Examples

The following example defines a range of on-demand Frame Relay circuits that will use the RADIUS servers in the `local` context to configure the circuits when activity is detected. A prefix-string of `first-dsl` is configured:

```
[local]RedBack(config-port)#frame-relay pvc on-demand 100 through 999 aaa context local
prefix-string first-dsl
```

Related Commands

frame-relay profile
frame-relay pvc
frame-relay pvc explicit
show frame-relay profile
show frame-relay pvc

frame-relay-test

frame-relay-test *slot/port* [**byte** *pattern*] [**packet** *count*] [**size** *bytes*] [**details**]

Purpose

Sends a test pattern out a particular Frame Relay port.

Command Mode

administrator exec

Syntax Description

slot/port	Backplane slot number and the specific port number.
byte *pattern*	Optional. Value of each byte in the test packet. The range of values is 0 to 255; the default value is 0. You can also enter this value in hexadecimal (0x0 to 0xFF).
packet *count*	Optional. Number of packets to transmit. The range of values is 1 to 100,000; the default is 1,000.
size *bytes*	Optional. Number of bytes in each test packet. The range of values is 20 to 8,000; the default is 100.
details	Optional. Enables the display of additional error details.

Default

Sends 1,000 100-byte packets with a pattern of all zeros.

Usage Guidelines

Use the **frame-relay-test** command in conjunction with the **loopback** command to test and debug a Frame Relay line. Use this command in conjunction with remote loopback to test connectivity with a remote node. You can stop the test by entering **Ctrl+C**.

Examples

The following example tests the connectivity to the Frame Relay node attached to slot 7 port 1. First, the port is configured for remote loopback. Next, the **frame-relay-test** command sends 10 test packets to be looped back by the remote system:

```
[local]RedBack(config)#port ds3 7/1
[local]RedBack(config-port)#framing c-bit
[local]RedBack(config-port)#loopback remote

Sending 5, 100-byte packets on port 7/1 with a test pattern of 0x55
sending remote loopback confirmation
remote loopback confirmation received
[local]RedBack(config-port)end
[local]RedBack#frame-relay-test 7/1 packet 10

Sending 10, 100-byte packets on port 7/1 with a test pattern of 0
!!!!!!!!!!
10 packets sent with pattern 0, 10 good packets received
0 packets with wrong length, 0 packets with bad data
```

Related Commands

loopback
show port info

radius attribute medium-type

radius attribute medium-type {**dsl** | **cable** | **wireless** | **satellite**}

{**no** | **default**} **radius attribute medium-type**

Purpose

Specifies the value that the Access Operating System (AOS) supplies for the Medium-Type vendor-specific attribute (VSA) in Remote Access Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets.

Command Mode

Frame Relay profile configuration

Syntax Description

dsl	Specifies that the value of the Medium-Type VSA is dsl.
cable	Specifies that the value of the Medium-Type VSA is cable.
wireless	Specifies that the value of the Medium-Type VSA is wireless.
satellite	Specifies that the value of the Medium-Type VSA is satellite.

Default

Sending of the Medium-Type attribute is disabled.

Usage Guidelines

Use the **radius attribute medium-type** command to specify the value of the Medium-Type attribute for any circuits that reference the profile.

Use the **no** or **default** form of this command to disable the sending of the attribute.

Note This command is also described in Chapter 41, “RADIUS Commands”.

Examples

The following example creates a Frame Relay profile named `FR-profile` and configures the Medium-Type attribute as `dsl`. If RADIUS Accounting is enabled, the PVCs in port `4/0` that reference this profile will have Accounting packets with the Medium-Type attribute containing the value `dsl`. Similarly, the attribute is present in Access-Request packets when attempting to authenticate Point-to-Point Protocol (PPP) users via RADIUS.

```
[local]RedBack(config)#frame-relay profile FR-profile
[local]RedBack(config-frpro)#counters
[local]RedBack(config-frpro)#radius attribute medium-type dsl
[local]RedBack(config-frpro)#exit
[local]RedBack(config)#port ds3 4/0
[local]RedBack(config-port)#frame-relay pvc 100 through 200 profile FR-profile
encapsulation ppp

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
[local]RedBack(config-pvc)#bind authentication chap pap
```

Related Commands

aaa accounting

show frame-relay counters

show frame-relay counters [**all**] [**profile** *prof-name*] [*slot/port* [**hdlc-channel** *chan-name*] [*dlci*] [**through** *end-dlci*]] [**no-counters** | **summary** | **details**] [**congestion**]

Purpose

Displays a list of traffic counters for configured Frame Relay permanent virtual circuits (PVCs).

Command Mode

operator exec

Syntax Description

all	Optional. Shows information for all configured Frame Relay PVCs. This option is valid only in the local context.
profile *prof-name*	Optional. Name of a Frame Relay profile for which counters are displayed.
slot/port	Optional. Backplane slot number and port number of a Frame Relay port for which counters are displayed.
hdlc-channel *chan-name*	Optional. Name of the High-level Data Link Control (HDLC) channel for which counters are displayed. This keyword and argument are required for channelized DS-3 ports and not allowed in any other case.
dlci	Optional. Data-link connection identifier (DLCI) of a configured PVC for which to display counters. The range of values is 16 to 991.
through *end-dlci*	Optional. Last DLCI when a range of DLCIs is requested.
summary	Optional. Shows only a summary of bound and unbound PVCs.
details	Optional. Specifies that more details are shown for each PVC.
no-counters	Optional. Specifies that only PVCs that do not have counters enabled are shown.
congestion	Optional. Specifies that only PVCs that have nonzero congestion counters are shown.

Default

Displays the counters for all Frame Relay PVCs that are bound in the current context.

Usage Guidelines

Use the **show frame-relay counters** command to display a list of traffic counters for configured Frame Relay circuits. Per-PVC traffic statistics are not kept by the system by default. Use the **counters** Frame Relay profile configuration command to enable statistics collection.

In the local context, specify the **all** keyword to display the counters for all configured Frame Relay PVCs, both bound (any context) and unbound. This option is only valid in the local context. For any other context, only PVCs bound within the current context are displayed.

Use the **profile** *prof-name* construct to show only PVCs that are configured with the specified profile.

Use the *slot/port* argument to show only PVCs configured on that slot and port. If the slot and port support HDLC channels, use the **hdlc-channel** *chan-name* construct to show only the counters for a specific channel. Otherwise, the counters for all PVCs on all HDLC channels on that slot/port are shown.

Use the *dlci* argument to show only a single PVC. Use the *dlci* **through** *end-dlci* construct to show counters for the specified range of DLCIs.

Use the **summary** keyword to display only a summary of counters; per-PVC counters are not shown.

Use the **details** keyword to show detailed output for each specified PVC; otherwise, the output displays one-line output for each PVC.

Use the **no-counters** keyword to show only the PVCs that do not have counters enabled.

Use the **congestion** keyword to show only the PVCs with nonzero congestion counters.

You can combine the optional keywords to show specific PVCs. For example, the **show frame-relay counters profile frame-1 2/0 20 through 30 details** command shows detailed counter information for DLCIs `20` through `30` on slot/port `2/0` that are configured with a profile of `frame-1` in the current context. If no counters had been enabled for profile `frame-1`, no PVCs are shown.

Examples

The following example displays the counters for all circuits:

```
[local]RedBack>show frame-relay counters all

WED JUL 28 10:03:57 1999
Slot                                                          Xmt Pkts
Port Channel  DLCI  Pkts Rcvd  Pkts Sent  Bytes Rcvd  Bytes Sent  Dropped
---- -------  ----  ---------  ---------  ----------  ----------  -------
 3/0            20        508          0       16256           0        0
 3/1            20          0        508           0       16256        0
pvcs with counters: 2           pvcs without counters: 0
pkts rcvd:  508                 pkts sent:  508          dropped: 0
bytes rcvd: 16256               bytes sent: 16256
```

The following example displays the counters only for the indicated circuit:

```
[local]RedBack>show frame-relay counters 3/1 20

Slot/Port: 3/1  DLCI: 20  profile: abc
status: UP      bound to b@a
first created: TUE JUL 27 15:45:07 1999
```

```
status change: TUE JUL 27 16:15:02 1999
last cleared:  never
pkts rcvd:  0               pkts sent:  510        dropped: 0
bytes rcvd: 0               bytes sent: 16320
FECNs rcvd: 0               BECNs rcvd: 0
DEs rcvd:   0               DEs sent:   0          discards:0
```

Related Commands

counters
frame-relay profile
frame-relay pvc
show frame-relay lmi-config
show frame-relay lmi-errors
show frame-relay lmi-stats
show frame-relay multicast
show frame-relay profile
show frame-relay pvc

show frame-relay lmi-config

show frame-relay lmi-config [*slot/port*]

Purpose

Displays the Local Management Interface (LMI) configuration.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a Frame Relay port.

Default

Displays the LMI configuration information for all configured Frame Relay ports.

Usage Guidelines

Use the **show frame-relay lmi-config** command to display LMI configuration information. If you specify the *slot/port* argument, the display shows the configuration for just that port.

Examples

The following example displays the configuration for a single port:

```
[local]RedBack>show frame-relay lmi-config 7/0

Slot                              Keep --------DCE-------- -- DTE --
Port Dlci Link Type      State    Alive T392 N391 N392 N393 N392 N393
---- ---- ---- ----      -----    ----- ---- ---- ---- ---- ---- ----
 7/0    0  DTE Ansi_AnxD DOWN        10   15    6    3    4    3    4
```

The following example displays the configuration for all configured ports:

```
[local]RedBack>show frame-relay lmi-config

Slot                              Keep --------DCE-------- -- DTE --
Port Dlci Link Type      State    Alive T392 N391 N392 N393 N392 N393
---- ---- ---- ----      -----    ----- ---- ---- ---- ---- ---- ----
 7/0    0  DTE Ansi_AnxD DOWN        10   15    6    3    4    3    4
 7/1    0  DCE ITU_AnxA  DOWN        10   15    6    3    4    3    4
```

Related Commands

frame-relay intf-type
frame-relay keepalive
frame-relay lmi-n391dte
frame-relay lmi-n392dce
frame-relay lmi-n392dte
frame-relay lmi-n393dce
frame-relay lmi-n393dte
frame-relay lmi-t392dce
frame-relay lmi-type

show frame-relay lmi-errors

show frame-relay lmi-errors [*slot/port*] [**full**]

Purpose

Displays Local Management Interface (LMI) error statistics.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a Frame Relay port.
full	Optional. Displays both Data Terminal Equipment (DTE) and Data Communications Equipment (DCE) error statistics.

Default

Displays LMI error statistics for all Frame Relay ports.

Usage Guidelines

Use the **show frame-relay lmi-errors** to display LMI error statistics. If you specify the *slot/port* argument, only counters for that slot/port are displayed.

The system maintains three sets of error counters for each LMI interface. There are general errors that apply regardless of the LMI interface type, error counters that only apply to the DCE interface, and error counters that only apply to the DTE interface.

When the error statistics are displayed, the general errors are always shown. Then normally the error counters for only the configured LMI interface type are displayed. For example, if port is configured with a Frame Relay interface type of DCE, only the DCE error counters would be displayed.

Both the DTE and DCE error counters are displayed in two cases:

- If the LMI interface type is network-to-network interface (NNI)
- If you specify the **full** keyword for the **show frame-relay lmi-errors** command

Examples

The following example displays the LMI errors for a single port:

```
[local]RedBack>show frame-relay lmi-errors 3/0

Port 3/0  General Errors       Last cleared: never
Header errors:         0       Protocol  errors:           0
Unknow Messages:       0       Invalid Unnumberd frame:    0
Frame too big:         0       Status rcvd for unkn pvc:   0
Too Many Status Enq:   0       Unexpected PVC Stat IE:     0
Too Few Stat Enq:      0       No response to Stat Enq:    0

Port 3/0  DTE LMI errors
Q.922 Header errors:   0       Protocol errors:            0
Unknown Messages:      0       Info Element missing:       0
KeepAlive IE Missing:  0       KeepALive Seq errors:       0
Unknown IE errors:     0       Positive Threshold Events:  0
Total Negative Events: 0       Current Threshold state:    Normal
```

Related Commands

frame-relay intf-type
show frame-relay lmi-config
show frame-relay lmi-stats

show frame-relay lmi-stats

show frame-relay lmi-stats [*slot/port*]

Purpose

Displays Local Management Interface (LMI) statistics.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Backplane slot number and port number of a Frame Relay port.

Default

Displays LMI statistics for all configured Frame Relay ports.

Usage Guidelines

Use the **show frame-relay lmi-stats** command to display LMI statistics. If you specify the *slot/port* argument, the LMI statistics for just that port are displayed.

Examples

The following example shows LMI statistics information for all Frame Relay ports:

```
[local]RedBack>show frame-relay lmi-stats

MON AUG 09 15:29:30 1999

LMI stats for port 2/0          Last cleared: never
status enquires sent:      396  status enquires rcvd:       0
full status enqs sent:      67  full status enqs rcvd:      0
status messages sent:        0  status messages rcvd:     395
full status msgs sent:       0  full status msgs rcvd:     67
                                async updates rcvd:         0

LMI stats for port 7/1          Last cleared: never
status enquires sent:        0  status enquires rcvd:     395
full status enqs sent:       0  full status enqs rcvd:     66
```

```
status messages sent:      395  status messages rcvd:       0
full status msgs sent:      67  full status msgs rcvd:      0
                                async updates rcvd:         0
```

Related Commands

show frame-relay lmi-config
show frame-relay lmi-errors

show frame-relay multicast

show frame-relay multicast [**all**] [**profile** *prof-name*] [*slot/port* [**hdlc-channel** *chan-name*] [*dlci*] [**through** *end-dlci*]] [**no-counters** | **summary** | **details**]

Purpose

Displays a list of traffic counters for Frame Relay permanent virtual circuits (PVCs).

Command Mode

operator exec

Syntax Description

all	Optional. Displays information on all configured Frame Relay PVCs. This option is valid only in the local context.
profile *prof-name*	Optional. Name of a Frame Relay profile.
slot/port	Optional. Backplane slot number and port number of a Frame Relay port.
hdlc-channel *chan-name*	Optional. Name of the High-level Data Link Control (HDLC) channel. This construct is valid only for channelized DS-3 ports.
dlci	Optional. Data-link connection identifier (DLCI) of a configured PVC. The range of values is 16 to 991.
through *end-dlci*	Optional. Last DLCI number in a range of DLCIs.
summary	Optional. Shows only a summary of bound and unbound PVCs.
details	Optional. Shows detailed per-PVC statistics.
no-counters	Optional. Shows PVCs that do not have counters enabled.

Default

Displays multicast counters for all Frame Relay PVCs that are bound in the current context.

Usage Guidelines

Use the **show frame-relay multicast** command to display multicast counters. Per-PVC traffic statistics are not kept by the system by default. Use the **counters** Frame Relay profile configuration command to enable statistics collection.

Use the **all** keyword to display multicast counters for all configured Frame Relay PVCs, both bound (any context) and unbound. This option is only valid in the local context. For any other context, only PVCs bound within the current context are displayed.

Use the **profile** *prof-name* construct to show only PVCs configured with the specified profile.

Use the *slot/port* argument to show only PVCs configured on that slot and port. If the slot and port support HDLC channels, use the **hdlc-channel** *chan-name* construct to show only the multicast counters for PVCs on that channel. Otherwise, multicast counters for all PVCs on all HDLC channels on that slot/port are shown.

Use the *dlci* argument to show a specific PVC. Use the *dlci* **through** *end-dlci* construct to show multicast counter information for the specified range of DLCIs.

Use the **summary** keyword to exclude per-PVC multicast counters and display only a summary.

Use the **details** keyword to display detailed output for each specified PVC; otherwise, the output displays one-line output for each PVC.

Use the **no-counters** keyword to display only the PVCs that do not have multicast counters enabled .

You can combine the optional keywords to show specific PVCs. For example, the **show frame-relay multicast profile frame-1 2/0 20 through 30 details** command shows detailed multicast counter information for DLCIs `20` through `30` on slot/port `2/0` that were configured with a profile of `frame-1` in the current context. If no multicast counters had been enabled for profile `frame-1`, no PVCs are shown.

Examples

The following example displays multicast statistics for all PVCs bound to interfaces and contexts with IGMP proxy enabled:

```
[local]RedBack>show frame-relay multicast

Slot                Multicast  Multicast  Multicast    Multicast
Port Channel DLCI   Pkts Rcvd  Pkts Sent  Bytes Rcvd   Bytes Sent
---- ------- ----   ---------  ---------  ----------   ----------
6/0            21           2          0          56            0
6/0            22           1          0          28            0
6/0            30           2          0          56            0
pvcs with mcast counters:3    pvcs without mcast counters: 0
multcast pkts rcvd:5          multicast pkts sent: 0
multicast bytes rcvd:140      multicast bytes sent: 0
```

The following example displays multicast statistics for the specified DLCI:

```
[local]RedBack>show frame-relay multicast 6/0 21

Slot/Port: 6/0  DLCI: 21      profile: mcast_fr
status: UP      bound to fr01@recv
first created: MON JUL 17 18:01:04 1999
status change: MON JUL 17 18:20:15 1999
last cleared:  never
multcast pkts rcvd:3          multicast pkts sent: 0
multicast bytes rcvd:84       multicast bytes sent: 0
```

The following example shows multicast details for all PVCs:

```
[local]RedBack>show frame-relay multicast details

TUE JUL 17 22:17:34 1999
Slot/Port: 6/0  DLCI: 21      profile: mcast_fr
status: UP      bound to fr01@recv
first created: MON JUL 17 18:01:04 1999
status change: MON JUL 17 18:20:15 1999
last cleared:  never
multcast pkts rcvd:3          multicast pkts sent: 0
multicast bytes rcvd:84       multicast bytes sent: 0

Slot/Port: 6/0  DLCI: 22     profile: mcast_fr
status: UP     bound to fr02@recv
first created: MON JUL 17 18:01:04 1999
status change: MON JUL 17 18:20:15 1999
last cleared:  never
multcast pkts rcvd:2          multicast pkts sent: 0
multicast bytes rcvd:56       multicast bytes sent: 0

Slot/Port: 6/0  DLCI: 30     profile: mcast_fr
status: UP     bound to rin1@recv
first created: MON JUL 17 18:01:04 1999
status change: MON JUL 17 18:20:15 1999
last cleared:  never
multcast pkts rcvd:4          multicast pkts sent: 0
multicast bytes rcvd:112      multicast bytes sent: 0

TUE JUL 06 22:17:34 1999
pvcs with mcast counters:3    pvcs without mcast counters: 0
multicast pkts rcvd:9         multicast pkts sent:0
multicast bytes rcvd:252      multicast bytes sent:0
```

The following example displays a brief summary of multicast statistics:

```
[local]RedBack>show frame-relay multicast summary

TUE JUL 17 22:17:34 1999
pvcs with mcast counters:3    pvcs without mcast counters: 0
multicast pkts rcvd:9         multicast pkts sent:0
multicast bytes rcvd:252      multicast bytes sent:0
```

Related Commands

counters
frame-relay profile
frame-relay pvc
show frame-relay counters

show frame-relay profile

show frame-relay profile [*prof-name*]

Purpose

Displays Frame Relay traffic management parameters.

Command Mode

operator exec

Syntax Description

prof-name	Optional. Name of a Frame Relay profile.

Default

Displays a list of all configured Frame Relay profiles.

Usage Guidelines

Use the **show frame-relay profile** command to display Frame Relay profile configuration information. Include the optional *prof-name* argument to show a detailed listing for the specified profile; otherwise, the output includes a summary listing of all Frame Relay profiles.

Examples

The following example shows sample output of the summary listing:

```
[local]RedBack>show frame-relay profile

MON AUG 09 16:25:10 1999
Name         Counters   Buffers
------------ --------   -------
abc          none       default
frame20      l2         default
mcast_fr     l2mc       default
```

The counters are specified as:

- none—no counters were specified in the profile
- l2—counters l2 (layer 2) was specified in the profile

- mc—counters multicast was specified in the profile
- l2mc—both l2 and multicast were specified in the profile

Related Commands

counters
frame-relay profile

show frame-relay pvc

show frame-relay pvc [**all**] [**profile** *prof-name*] [*slot/port* [**hdlc-channel** *chan-name*] [*dlci* [**through** *end-dlci*]]] [**summary** | **up** | **down**]

Purpose

Displays a list of configured Frame Relay permanent virtual circuits (PVC)s.

Command Mode

operator exec

Syntax Description

all	Optional. Shows information for all configured Frame Relay PVCs. This option is valid only in the local context.
profile *prof-name*	Optional. Name of a Frame Relay profile to limit the display to.
slot/port	Optional. Backplane slot number and port number of a Frame Relay port.
hdlc-channel *chan-name*	Optional. Name of a High-level Data Link Control (HDLC) channel. This construct is valid only for channelized DS-3 ports.
dlci	Optional. Data-link connection identifier (DLCI) of the configured PVC or the first DLCI when information on a range is being requested. The range of values is 16 to 991.
through *end-dlci*	Optional. Last DLCI when a information on a range of DLCIs is being requested.
summary	Optional. Shows only a summary of bound and unbound PVCs.
up	Optional. Shows only active PVCs.
down	Optional. Shows only inactive PVCs.

Default

Displays all configured Frame Relay PVCs that are bound in the current context.

Usage Guidelines

Use the **show frame-relay pvc** command to display information on Frame Relay PVCs. In the local context, use the **all** keyword to display information about all configured Frame Relay PVCs, both bound (in any context) and unbound. This option is valid only in the local context. For any other context, only PVCs that are bound within the current context are displayed.

Use the **profile** *prof-name* construct to show only PVCs configured with that profile.

Use the *slot/port* argument to show only PVCs for that port. If the slot and port support HDLC channels, use the **hdlc-channel** *chan-name* construct to show only the PVCs on that channel; otherwise, the PVCs on all HDLC channels on the port are shown.

Use the *dlci* argument to show only that PVC. Use the *dlci* **through** *end-dlci* construct to show a range of PVCs.

For any PVC for which encapsulation auto-detection is enabled (in other words, the encapsulation type is set to **auto1490** or **ppp auto**), the display shows the PVC encapsulation type as **auto** *type* until the actual encapsulation type has been detected. Once the encapsulation type has been detected, the display shows the specific PPP or RFC 1490 encapsulation type (for example, **bridge1490**).

Use the **summary** keyword to display only summary information.

Use the **up** keyword to display only the active PVCs; use the **down** keyword to display only the inactive PVCs.

Examples

The following examples display sample output of the **show frame-relay pvc** command, where counters (in the Ctrs column) are specified as:

- none—no counters were specified in the profile
- l2—**counters l2** (layer 2) was specified in the profile
- mc—**counters multicast** was specified in the profile
- l2mc—both **l2** and **multicast** were specified in the profile

```
[local]RedBack>show frame-relay pvc all

MON JUL 26 18:41:35 1999
Port Channel DLCI  Traffic Profile State Ctrs  Encaps     Binding
---- ------- ----  --------------- ----- ----  ---------- -------
 7/0           16  fr                UP   l2  route1490  fr1@fr2
 7/0           77  abc             DOWN none  ppp
 7/0           78  abc             DOWN none  ppp
 7/0           79  frame           DOWN   l2  ppp
 7/0           80  frame           DOWN   l2  ppp
 7/0          100  frame             UP   l2  bridge1490 fr1@frame
 7/1           16  fr                UP   l2  route1490  fr2@fr1
 7/1           55  frame             UP   l2  multi      by1@b
 7/1           56  frame             UP   l2  route1490  by2@b
 7/1           58  frame             UP   l2  route1490  by1@b
 7/1           60  frame             UP   l2  bridge1490 by1@a
 7/1          100  frame             UP   l2  bridge1490 fr1@frame2
circuits up: 8  circuits down: 4  total circuits: 12
```

The following example displays multicast statistics for slot 6/port 1 for the DLCI range 21 through 30:

```
[local]RedBack>show frame-relay pvc 6/1 21 through 30

TUE JUL 06 22:20:21 1999
Port Channel DLCI  Traffic Profile State Ctrs  Encaps     Binding
---- ------- ----  ------- ------- ----- ----  ------     -------
6/1            21  mcast_fr           UP l2mc  route1490  fr01@recv
6/1            22  mcast_fr           UP l2mc  route1490  fr02@recv
6/1            30  mcast_fr           UP l2mc  route1490  rin[recv]
circuits up: 3 circuits down: 0 total circuits: 3
```

The following example displays information for the PVC associated with slot 7 port 1, DLCI 16:

```
[local]RedBack>show frame-relay pvc 7/1 16

Slot/Port: 7/1  DLCI: 16  profile: fr
status: UP      bound to fr2@fr1
first created: FRI JUL 09 02:42:55 1999
status change: FRI JUL 09 02:42:59 1999
last cleared:  never
pkts rcvd:  1                pkts sent:  1            dropped: 0
bytes rcvd: 38               bytes sent: 38
FECNs rcvd: 0                BECNs rcvd: 0
DEs rcvd:   0                DEs sent:   0            discards:0
```

Related Commands

counters
frame-relay pvc
show frame-relay profile

802.1Q Commands

This chapter describes the commands used to configure the 802.1Q encapsulation feature supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure 802.1Q, and configuration examples, see the “Configuring 802.1Q” chapter in the *Access Operating System (AOS) Configuration Guide*.

description

description *text*

no description

Purpose

Assigns a textual description to an 802.1Q permanent virtual circuit (PVC).

Command Mode

dot1q PVC configuration

Syntax Description

text	Text string that identifies the port. Can be any alphanumeric string, including spaces. The text cannot exceed a single line.

Default

No description is associated with a circuit.

Usage Guidelines

Use the **description** command to associate additional information with the name of the circuit.

Use the **no** form of this command to delete a previously created description. To change a description, simply create a new one and it overwrites the existing one.

Examples

The following example configures a description for the 802.1 PVC for VLAN ID 44:

```
[local]RedBack(config-port)#dot1q pvc 44
[local]RedBack(config-dot1q-pvc)#description to DSLAM in Rack 5, Shelf 4
```

Related Commands

dot1q profile

dot1q profile *prof-name*

no dot1q profile *prof-name*

Purpose

Creates an 802.1Q profile if it does not already exist, and enters dot1q profile configuration mode.

Command Mode

global configuration

Syntax Description

prof-name	Name of the 802.1Q profile.

Default

No dot1q profiles are defined.

Usage Guidelines

Use the **dot1q profile** command to create or modify an 802.1Q profile. You must create a dot1q profile before you can create any 802.1Q PVCs.

Use the **no** form of this command to delete an 802.1Q profile.

Examples

The following example creates an 802.1Q profile named `1q-prof`:

```
[local]RedBack(config)#dot1q profile 1q-prof
[local]RedBack(config-dot1qpro)#
```

Related Commands

dot1q pvc
show dot1q profile

dot1q pvc

dot1q pvc {*vlan-id* [**through** *end-vlan-id*] | **untagged**} **profile** *prof-name* **encapsulation** {**ipoe** | **multi** | **pppoe**}

no dot1q pvc {*vlan-id* | **untagged**}

Purpose

Creates an 802.1Q permanent virtual circuit.

Command Mode

circuit configuration
port configuration

Syntax Description

vlan-id	802.1Q virtual LAN (VLAN) tag value. The range of values is 2 to 4,094.
through *end-vlan-id*	VLAN tag of the last VLAN in the range.
untagged	Specifies configuration for untagged traffic.
profile *prof-name*	Name of the 802.1Q profile to use for the circuit.
encapsulation	Specifies the encapsulation type (from the keywords that follow).
ipoe	Specifies that the circuit carries IP over Ethernet traffic.
multi	Specifies that the circuit carries both IP over Ethernet and Point-to-Point Protocol over Ethernet (PPPoE) traffic.
pppoe	Specifies that the circuit carries PPPoE traffic.

Default

No 802.1Q PVCs are defined.

Usage Guidelines

Use the **dot1q pvc** command to create an 802.1Q circuit on an Ethernet port, Asynchronous Transfer Mode (ATM) circuit, or Frame Relay circuit. The circuit can carry IP over Ethernet traffic, PPPoE traffic, or a mixture of both types of traffic, depending on the selected encapsulation.

Note You cannot create 802.1Q PVCs on the Ethernet Management port.

Use the **no** form of this command to delete an 802.1Q PVC.

Examples

The following example creates a dot1q PVC for VLAN ID `20`, and uses the profile named `1q-prof`, on an Ethernet port:

```
[local]RedBack(config)#port ethernet 3/0
[local]RedBack(config-port)#encapsulation dot1q
[local]RedBack(config-port)#dot1q pvc 20 profile 1q-prof encapsulation multi
[local]RedBack(config-dot1q-pvc)#
```

Related Commands

dot1q profile

pbit-setting

pbit-setting *value*

default pbit-setting

Purpose

Assigns a value for the three 802.1P priority bits in the 802.1Q header on all 802.1Q circuits that reference the profile.

Command Mode

dot1q profile configuration

Syntax Description

value	Hexadecimal value for the p-bits. The range of values is 0 to 7.

Default

The default priority bit setting is 0.

Usage Guidelines

Use the **pbit-setting** command to specify the setting for the priority bits in the 802.1Q header for all 802.1Q circuits that reference this profile.

Use the **default** form of this command to return the p-bit setting to the default value.

Examples

The following example sets the p-bit value to 5:

```
[local]RedBack(config-dot1qpro)#pbit-setting 5
```

Related Commands

dot1q pvc
show dot1q profile

show dot1q counters

show dot1q counters [**all**] [**profile** *prof-name*] [*slot/port* [**hdlc-channel** *chan-name*] [{**all** | *vpi* [**through** *end-vpi* | *vci* [**through** *end-vci*]] | *dlci* [**through** *end-dlci*]} [**dot1q-pvc** {*vlan-id* [**through** *end-vlan-id*] | **untagged**}]]] [**summary**]

Purpose

Displays counters for 802.1Q permanent virtual circuits (PVCs).

Command Mode

operator exec

Syntax Description

all	Optional. Displays 802.1Q PVCs in all contexts. Without this keyword, displays only PVCs in the current context.
profile *prof-name*	Optional. Name of the 802.1Q profile for which associated PVCs are displayed.
slot/port	Optional. Backplane slot and port number for which PVCs are displayed.
hdlc-channel *chan-name*	Optional. Name of the HDLC channel for which PVCs are displayed. This construct is allowed only for channelized DS-3 ports.
all	Optional. Displays 802.1Q PVCs on all circuits on the port.
vpi	Optional. Virtual path identifier (VPI) for which PVCs are displayed. The range of values is 0 to 255.
through *end-vpi*	Optional. Last VPI when displaying 802.1Q PVCs on a range of ATM virtual paths.
vci	Optional. Virtual channel identifier (VCI) for which PVCs are displayed. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when displaying 802.1Q PVCs on a range of ATM circuits.
dlci	Optional. Data Link Connection Identifier for which 802.1Q PVCs are displayed. The range of values is 16 to 991.
through *end-dlci*	Optional. Last DLCI when displaying 802.1Q PVCs on a range of Frame Relay circuits.

dot1q-pvc	Optional. Displays specific 802.1Q PVCs with the specified Virtual LAN (VLAN) tag identifiers.
vlan-id	VLAN tag id for an 802.1Q PVC to be displayed, or the first VLAN tag id in a range of 802.1Q PVCs to be displayed. The range of values is 2 to 4,094.
through *end-vlan-id*	Optional. Last VLAN ID when displaying a range of 802.1Q PVCs.
untagged	Displays statistics for untagged 802.1Q PVCs.
summary	Optional. Displays only summary counters for the selected 802.1Q PVCs.

Default

Displays counters for all 802.1Q PVCs in the current context.

Usage Guidelines

Use the **show dot1q counters** command in operator exec mode to display counters for 802.1Q PVCs.

Examples

The following example displays all 802.1Q PVCs on port 7/1:

```
[local]RedBack>show dot1q counters all 7/1

MON APR 30 13:34:42 2001
Slot
Port Channel  Vlan  Pkts Rcvd  Pkts Sent  Bytes Rcvd  Bytes Sent
---- -------  ----  ---------  ---------  ----------  ----------
 7/1           16
              2             0          0           0             0
 7/1           20
              2             0          0           0             0
              3             0          0           0             0
total dot1q pvcs:3
pkts rcvd:  0                   pkts sent:  0
bytes rcvd: 0                   bytes sent: 0
```

Related Commands

dot1q pvc
show dot1q pvc

show dot1q profile

show dot1q profile [*prof-name*]

Purpose

Displays 802.1Q profiles defined on the system.

Command Mode

operator exec

Syntax Description

prof-name	Optional. Name of a specific profile to display.

Default

Displays all 802.1Q profiles.

Usage Guidelines

Use the **show dot1q profile** command to display all 802.1Q profiles defined on the system or a specific 802.1Q profile.

Examples

The following example shows sample output from the **show dot1q profile** command:

```
[local]RedBack>show dot1q profile

MON APR 30 13:41:30 2001

Name         Pbits
------------ -----
802prof1     0
802prof2     7
```

Related Commands

dot1q profile

show dot1q pvc

show dot1q pvc [**all**] [**profile** *prof-name*] [*slot/port* [**hdlc-channel** *chan-name*] [{**all** | *vpi* [**through** *end-vpi* | *vci* [**through** *end-vci*]] | *dlci* [**through** *end-dlci*]} [**dot1q-pvc** {*vlan-id* [**through** *end-vlan-id*] | **untagged**}]]] [**up** | **down** | **summary**]

Purpose

Displays information on 802.1Q permanent virtual circuits.

Command Mode

operator exec

Syntax Description

all	Optional. Displays 802.1Q PVCs in all contexts. Without this keyword, displays only PVCs in the current context.
profile *prof-name*	Optional. Name of the 802.1Q profile for which associated PVCs are displayed.
slot/port	Optional. Backplane slot and port number for which PVCs are displayed.
hdlc-channel *chan-name*	Optional. Name of the HDLC channel for which PVCs are displayed. This construct is allowed only for channelized DS-3 ports.
all	Optional. Displays 802.1Q PVCs on all circuits on the port.
vpi	Optional. Virtual path identifier (VPI) for which PVCs are displayed. The range of values is 0 to 255.
through *end-vpi*	Optional. Last VPI when displaying 802.1Q PVCs on a range of ATM virtual paths.
vci	Optional. Virtual channel identifier (VCI) for which PVCs are displayed. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when displaying 802.1Q PVCs on a range of ATM circuits.
dlci	Optional. Data Link Connection Identifier for which 802.1Q PVCs are displayed. The range of values is 16 to 991.
through *end-dlci*	Optional. Last DLCI when displaying 802.1Q PVCs on a range of Frame Relay circuits.

dot1q-pvc	Optional. Displays specific 802.1Q PVCs with the specified Virtual LAN (VLAN) tag identifiers.
vlan-id	VLAN tag id for an 802.1Q PVC to be displayed, or the first VLAN tag id in a range of 802.1Q PVCs to be displayed. The range of values is 2 to 4,094.
through *end-vlan-id*	Optional. Last VLAN ID when displaying a range of 802.1Q PVCs.
untagged	Displays untagged 802.1Q PVCs.
up	Displays only 802.1Q PVCs that are up.
down	Displays only 802.1Q PVCs that are down.
summary	Optional. Displays only summary counters for the selected 802.1Q PVCs.

Default

Displays all 802.1Q PVCs that are bound in the current context.

Usage Guidelines

Use the **show dot1q pvc** command to display information on 802.1Q PVCs.

Examples

The following example sets the p-bit value to 5:

```
[local]RedBack>show dot1q pvc

MON APR 30 13:52:47 2001
Port Channel    Vlan Traffic Profile State Encaps Binding
---- --------   ---- --------------- ----- ------ -------
 2/1
                 40  802prof1        DOWN  ip     if1 [local]
                 41  802prof1        DOWN  ip     if1 [local]
                 42  802prof1        DOWN  ip     if1 [local]
                 43  802prof1        DOWN  ip     if1 [local]
                 44  802prof1        DOWN  ip     if1 [local]
                 45  802prof1        DOWN  ip     if1 [local]
                 46  802prof1        DOWN  ip     if1 [local]
                 47  802prof1        DOWN  ip     if1 [local]
                 48  802prof1        DOWN  ip     if1 [local]
                 49  802prof1        DOWN  ip     if1 [local]
                 50  802prof1        DOWN  ip     if1 [local]
 7/1           20
                  2  802prof2        DOWN  multi  xxx29.3.0.1@local
                  3  802prof2        DOWN  multi  xxx29.3.0.2@local
circuits up: 0  circuits down: 13  total circuits: 13
```

Related Commands

dot1q pvc
show dot1q counters

Bind Commands

This chapter describes the commands used to configure bindings for ports and circuits supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure AOS bindings, and configuration examples, see the “Configuring Bindings” chapter in the *Access Operating System (AOS) Configuration Guide*.

bind authentication

bind authentication {**pap** | **chap** [**wait**] | **chap pap** [**wait**]} [**maximum** *sessions*] [**context** *ctx-name* | **service-group** *svc-name*]

no bind authentication

Purpose

Dynamically binds the Point-to-Point Protocol (PPP)-encapsulated port, circuit, or channel to an interface using the specified PPP authentication protocol.

Command Mode

circuit configuration
dot1q PVC configuration
HDLC channel configuration
port configuration

Syntax Description

pap	Specifies that the PPP authentication protocol to be used is Password Authentication Protocol (PAP).
chap	Specifies that the PPP authentication protocol to be used is Challenge Handshake Authentication Protocol (CHAP).
chap pap	Specifies that either CHAP or PAP can be used.
wait	Optional. Specifies that the inbound CHAP authentication is completed first. Available only for the **chap** or **chap pap** keywords.
maximum *sessions*	Optional. Maximum number of concurrent sessions allowed on a circuit or port. The range of values is 1 to 4,000. This construct applies only to circuits and ports using PPP over Ethernet (PPPoE).
context *ctx-name*	Optional. Name of the context to which PPP sessions on the circuits and ports being bound are restricted.
service-group *svc-name*	Optional. Name of the service access list that defines the services available to the PPP-encapsulated circuit or port.

Default

None

Usage Guidelines

Use the **bind authentication** command to create a dynamic binding for the port, circuit, or channel, based on PPP session authentication information. This command is only valid on a port, circuit, or channel that has been previously configured to use one of the PPP encapsulation types.

You cannot bring up a PPP link until the username and password negotiations have been completed and authorization has been granted. The username string provided during PPP authentication is interpreted according to the rules in the **aaa username-format** commands and the **aaa default-domain** command.

Note The IP address configured for a subscriber, either in a local subscriber record or that obtained from a Remote Authentication Dial-In User Service (RADIUS) server, must fall within the range (address and network mask) of an interface defined within the context to which that subscriber is to be bound. Otherwise, the bind fails and the PPP-encapsulated circuit does not come up.

The optional **maximum** *sessions* construct is only relevant to circuits and ports using PPPoE. When using the optional **context** *ctx-name* construct, all attempts to bind PPP sessions to contexts other than the one specified fail. When using the optional **service-group** *svc-name* construct, all attempts to authenticate to contexts or domains not permitted by the named service access list fail.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example sets the encapsulation to PPP over HDLC and then binds the port using CHAP or PAP protocol:

```
[local]RedBack(config)#port ds3 4/1
[local]RedBack(config-port)#encapsulation ppp
[local]RedBack(config-port)#bind authentication chap pap
```

Related Commands

aaa default-domain
aaa username-format
encapsulation
service access-list

bind auto-subscriber

bind auto-subscriber *prefix1 ctx-name* [**password** *prefix2*]

no bind auto-subscriber *prefix1 ctx-name*

Purpose

Automatically generates a **bind subscriber** command with a unique subscriber name for each permanent virtual circuit (PVC) in a range of Asynchronous Transfer Mode (ATM) or Frame Relay PVCs.

Command Mode

circuit configuration

Syntax Description

prefix1	Leading text string for each subscriber name.
ctx-name	Name of the context to locate the subscriber information.
password *prefix2*	Optional. Leading text string for each subscriber password.

Default

None

Usage Guidelines

Use the **bind auto-subscriber** command in conjunction with the **atm pvc explicit**, **atm pvc through**, **frame-relay pvc explicit**, or **frame-relay pvc through** command to automatically generate **bind subscriber** commands with unique subscriber names and optional passwords for each circuit in the range.

Note You cannot use this command with a simple **atm pvc** or **frame-relay pvc** command (in other words, without the **through** construct), or with the **atm pvc on-demand** or **frame-relay pvc on-demand** command.

The generated subscriber names and passwords are of the following forms for ATM circuits:

subscriber name: *prefix1*slot.port.vpi.vci@*ctx-name*
password: *prefix2*slot.port.vpi.vci

The generated subscriber names and passwords are of the following forms for Frame Relay circuits:

subscriber name: *prefix1*slot.port.dlci@*ctx-name*
password: *prefix2*slot.port.dlci

Note The IP address configured for a subscriber, either in a local subscriber record or that obtained from a Remote Access Dial-In User Service (RADIUS) server, must fall within the range (address and network mask) of an interface defined within the context to which that subscriber is to be bound. Otherwise, the bind fails and the PPP-encapsulated circuit does not come up.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove all the automatically generated subscriber bindings with the specified prefix and context.

Examples

The following example creates 10 ATM PVCs with a virtual path identifier (VPI) value of `0`, and virtual channel identifier (VCI) values ranging from `100` to `109`, then uses the **bind auto-subscriber** command to bind each PVC to an automatically generated subscriber name beginning with the string `DSL`:

```
[local]RedBack(config)#port atm 2/1
[local]RedBack(config-port)#atm pvc 0 100 through 109 profile fast encapsulation
route1483
!!!!!!!!!!
[local]RedBack(config-pvc)#bind auto-subscriber DSL local
```

The example results in the following lines in the system configuration:

```
port atm 2/1
 atm pvc 0 100 profile fast encapsulation bridge1483
 bind subscriber DSL2.1.0.100@local
 atm pvc 0 101 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.101@local
 atm pvc 0 102 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.102@local
 atm pvc 0 103 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.103@local
 atm pvc 0 104 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.104@local
 atm pvc 0 105 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.105@local
 atm pvc 0 106 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.106@local
 atm pvc 0 107 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.107@local
 atm pvc 0 108 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.108@local
 atm pvc 0 109 profile fast encapsulation bridge1483
  bind subscriber DSL2.1.0.109@local
```

Related Commands

atm pvc
atm pvc explicit
atm pvc on-demand
bind subscriber
frame-relay pvc
frame-relay pvc explicit
frame-relay pvc on-demand

bind bypass

bind bypass *bypass-name ctx-name*

no bind bypass

Purpose

Statically associates a port, circuit or channel with a bypass.

Command Mode

circuit configuration
HDLC channel configuration
port configuration

Syntax Description

bypass-name	Name of a previously configured bypass to which the port is to be bound.
ctx-name	Name of the context where the bypass exists.

Default

None

Usage Guidelines

Use the **bind bypass** command to statically associates a port, circuit or channel with a bypass. This command is not valid in port configuration mode or High-level Data Link Control (HDLC) channel configuration mode for ports or channels with Frame Relay or Point-to-Point Protocol (PPP) encapsulation.

Note the following considerations:

- The two elements bound to the same bypass must have the same encapsulation type. For example, two ATM PVCs can bound to the same bypass if they both have RFC 1483 routed encapsulation.
- A Frame Relay PVC can only be bound to an ATM PVC if both PVCs use bridged encapsulation or both PVCs use routed encapsulation. The Access Operating System (AOS) can automatically convert between RFC 1483 bridged encapsulation and RFC 1490 bridged encapsulations, and RFC 1483 routed and RFC 1490 routed encapsulation.
- The two PVCs can reside on the same port or on different ports.
- No element being bound to a bypass can have PPP encapsulation.
- Once two PVCs are bound together, all incoming traffic from one PVC is sent out the other PVC. This means, for example, that if a ping is received on one PVC, it is not responded to by the local system; rather it is sent out the other PVC like all other traffic.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to eliminate the binding between a port, circuit, or channel and a bypass.

Examples

The following example binds the two ports in I/O slot 2 to the bypass named `fr_bypass` in the local context:

```
[local]RedBack(config)#port ds3 2/0
[local]RedBack(config-port)#encapsulation cisco-hdlc
[local]RedBack(config-port)#bind bypass fr_bypass local
[local]RedBack(config-port)#exit
[local]RedBack(config)#port ds3 2/1
[local]RedBack(config-port)#encapsulation cisco-hdlc
[local]RedBack(config-port)#bind bypass fr_bypass local
```

Related Commands

bypass
encapsulation
show bypass

bind dot1q

bind dot1q *slot/port vlan-tag-ID*

no bind dot1q *slot/port vlan-tag-ID*

Purpose

Provides static interworking between RFC 1483 bridged or RFC 1490 bridged-encapsulated permanent virtual circuits (PVCs) and 802.1Q-tagged Ethernet frames.

Command Mode

circuit configuration

Syntax Description

slot/port	Slot and port of the Ethernet port to which to bind.
vlan-tag-ID	Specific tag to which this PVC is mapped on the specified Ethernet port. The range of values is 2 to 4,094.

Default

None

Usage Guidelines

Use the **bind dot1q** command to bind an ATM or Frame Relay PVC to an Ethernet port using the specified VLAN ID. When this binding is in effect, AOS strips tagged traffic received on the Ethernet port and transmits the traffic over the PVC using the configured encapsulation. When traffic is received on the PVC, AOS adds the VLAN ID tag before forwarding the traffic on the Ethernet port.

This command only applies to RFC 1483 bridged ATM PVCs or RFC 1490 bridged Frame Relay PVCs. You can create a separate binding on the Ethernet port to handle untagged frames that arrive on the Ethernet port.

The **show bindings** command shows the mapping between PVCs and VLAN tags. You must be in the local context to show the bindings.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example uses the **bind interface** command to associate untagged frames that arrive over Ethernet port `2/0` with the local context, and the **bind dot1q** command to associated tagged frames (with VLAN ID `44`) on that same port with ATM PVC `0:31` on port `4/1`:

```
[local]RedBack(config)#port ethernet 2/0
[local]RedBack(config-port)#bind interface downstream local
[local]RedBack(config-port)#exit
[local]RedBack(config)#port atm 4/1
[local]RedBack(config-port)#atm pvc 0 31 profile ubr encapsulation bridge1483
[local]RedBack(config-pvc)#bind dot1q 2/0 44
```

Related Commands

show bindings

bind interface

bind interface *if-name ctx-name*

no bind interface

Purpose

Statically associates a port, circuit, channel, or Generic Routing Encapsulation (GRE) tunnel to the specified interface in the specified context.

Command Mode

circuit configuration
dot1q PVC configuration
HDLC channel configuration
port configuration
tunnel circuit configuration

Syntax Description

if-name	Name of a previously configured interface.
ctx-name	Name of the context in which the specified interface exists.

Default

None

Usage Guidelines

Use the **bind interface** command to statically associate a port, circuit, channel, or GRE tunnel to the specified interface in the specified context.

This command is only available in port configuration mode for Ethernet ports and dot1q PVCs when the encapsulation is set to IP over Ethernet. Only one Ethernet port can be bound to a routing interface, and vice-versa.

It is available for other ports, circuits and channels when the encapsulation is set to Cisco High-Level Data Link Control (HDLC).

Both the interface and the specified context must exist prior to executing the **bind interface** command. If either is missing, an error message is displayed.

modem circuit is bound.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example sets the encapsulation on a clear-channel DS-3 port to Cisco HDLC and binds the port to the interface `SoHo1` in the `local` context:

```
[local]RedBack(config)#port ds3 3/0
[local]RedBack(config-port)#encapsulation cisco-hdlc
[local]RedBack(config-port)#bind interface SoHo1 local
```

Related Commands

encapsulation

bind l2tp-tunnel

bind l2tp-tunnel *tun-name ctx-name*

no bind l2tp-tunnel

Purpose

Binds a Layer 2 Tunneling Protocol (L2TP)-encapsulated circuit to a specific tunnel within a context.

Command Mode

circuit configuration

Syntax Description

tun-name	Name of the tunnel to which the L2TP-encapsulated circuit is bound.
ctx-name	Name of the context in which the tunnel is configured.

Default

None

Usage Guidelines

Use the **bind l2tp** tunnel command to bind an L2TP-encapsulated circuit to a specific tunnel within a specific context.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example configures an ATM PVC on a system names `lac.com` and binds that PVC to the tunnel `lns.net` in the `local` context:

```
[local]lac.com(config)#port atm 4/1
[local]lac.com(config-port)#atm pvc 0 1 profile ubr encapsulation l2tp
[local]lac.com(config-pvc)#bind l2tp-tunnel lns.net local
```

Related Commands

encapsulation
l2tp-peer name
l2f-peer name

bind multi

bind multi {**interface** *if-name ctx-name* | **subscriber** *sub-name*} **authentication** {**pap** | **chap** [**wait**] | **chap pap** [**wait**]} [**maximum** *sessions*] [**context** *ctx-name* | **service-group** *svc-name*]

no bind

Purpose

Specifies the bindings for each of the encapsulations on a multiencapsulated port or circuit.

Command Mode

circuit configuration
dot1q PVC configuration
port configuration

Syntax Description

interface *if-name*	Name of the interface to which the IP over Ethernet portion of the circuit is to be bound.
ctx-name	Name of the context for the interface to which the IP over Ethernet portion of the circuit is to be bound.
subscriber *sub-name*	Username and domain name that define the subscriber record to be used. If a custom structured username format is configured, the format of the *sub-name* argument must match (see the **aaa default-domain** and **aaa username-format** commands). Otherwise, the *sub-name* argument must take the default form of *user@domain*. This keyword is not allowed in dot1q pvc configuration mode.
authentication	Specifies the binding for the PPP over Ethernet (PPPoE) portion of the circuit. Must be followed by the selection of an authentication protocol.
pap	Specifies that the Point-to-Point Protocol (PPP) authentication protocol to be used is Password Authentication Protocol (PAP).
chap	Specifies that the PPP authentication protocol to be used is Challenge Handshake Authentication Protocol (CHAP).
wait	Optional. Specifies that the inbound CHAP authentication is completed first. Available only with the **chap** or **chap pap** keywords.
chap pap	Specifies that either CHAP or PAP can be used.
maximum *sessions*	Optional. Maximum number of concurrent sessions allowed on a circuit or port. The maximum configurable value is the maximum number of subscribers allowed on the Subscriber Management System (SMS) device.

context *ctx-name*	Optional. Name of a specific context to which PPP sessions on the circuits and ports being bound are restricted.
service-group *svc-name*	Optional. Name of the service group that defines the services to which the PPP-encapsulated circuit or port are restricted.

Default

The multiple encapsulation feature is disabled.

Usage Guidelines

Use the **bind multi** command to enable multiple encapsulation types on the same port or circuit, and to define the binding for each encapsulation type. For Asynchronous Transfer Mode (ATM) circuits, the encapsulation types are RFC 1483 bridged and PPPoE; for Frame Relay circuits, the encapsulation types are RFC 1490 bridged and PPPoE; for Ethernet ports and dot1q PVCs, the encapsulation types are IP over Ethernet and PPPoE. You must configure the port, circuit, dot1q PVC, or channel for multiple encapsulations (using the **encapsulation** command, or the **multi** keyword for the **atm pvc** and **frame-relay pvc** commands).

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example creates an ATM PVC with multiple encapsulations. The IP over Ethernet traffic is bound to interface `downstream1` in the `local` context and the PPPoE traffic is bound through the results of `PAP` authentication, with a limit of `5` simultaneous PPPoE sessions:

```
[local]RedBack(config)#port atm 3/0
[local]RedBack(config-port)#atm pvc 1 32 profile ubr encapsulation multi
[local]RedBack(config-pvc)#bind multi interface downstream1 local authentication pap
maximum 5
```

The following example configures a Frame Relay PVC in a High-level Data Link Control (HDLC) channel of a channelized DS-3 port with multiple encapsulations. The IP over Ethernet traffic is bound to subscriber `user1` in the `local` context and the PPPoE traffic is bound through the results of `CHAP` authentication:

```
[local]RedBack(config)#port channelized-ds3 4/0
[local]RedBack(config-port)#hdlc-channel One t1 1 timeslot 1-24
[local]RedBack(config-chan)#encapsulation frame-relay
[local]RedBack(config-chan)#frame-relay pvc 100 profile frame1 encapsulation multi
[local]RedBack(config-pvc)#bind multi subscriber user1@local authentication chap
```

Related Commands

aaa default-domain
aaa username-format
atm pvc
encapsulation
frame-relay pvc

bind session

bind session *peer-name ctx-name* [**maximum** *sessions*] [**bridge-acl** *list-name*]

no bind session *peer-name*

Purpose

Binds the Point-to-Point Protocol (PPP) or Ethernet-encapsulated (including RFC 1483 bridged, RFC 1490 bridged, and Ethernet) port, High-level Data Link Control (HDLC) channel, dot1q PVC, or circuit to a specific Layer 2 Tunneling Protocol (L2TP), or Layer 2 Forwarding (L2F) peer, or L2TP group within a specific context.

Command Mode

circuit configuration
dot1q PVC configuration
HDLC channel configuration
port configuration

Syntax Description

peer-name	Name of the L2TP or L2F peer, or L2TP group to which the PPP-encapsulated port, HDLC channel, or circuit is to be bound.
ctx-name	Name of the context for the specified peer.
maximum *sessions*	Optional. Maximum number of concurrent sessions allowed on a circuit or port. The range of values is 1 to 8,000; the default is unlimited. This only applies to circuits and ports using PPP over Ethernet (PPPoE).
bridge-acl *list-name*	Optional. Name of the bridge access control list to be applied.

Default

None

Usage Guidelines

Use the **bind session** command to create a static binding of a PPP-encapsulated port, HDLC channel, dot1q PVC or circuit to a specific L2TP or L2F peer or to an L2TP group. This command disables dynamic tunnel selection for subscribers on the port, circuit, or channel.

This command is only available in port configuration mode and HDLC channel configuration mode when the encapsulation has been set to PPP.

Use the **bridge-acl** *list-name* construct to specify a bridge access control list to be applied to the session. The access control list must already have been configured in the specified context. This is typically used to filter packets so that only PPPoE traffic is allowed through an Ethernet over L2TP tunnel.

The optional **maximum** *sessions* construct is only relevant to circuits and ports using PPPoE.

An L2TP group name can be used as the *peer-name* argument.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example shows a port being bound to a tunnel named `isp2.net` in the local context:

```
[local]lac.telco.com(config-port)#encapsulation ppp
[local]lac.telco.com(config-port)#bind session isp2.net local
```

Related Commands

encapsulation
show bindings

bind subscriber

bind subscriber *sub-name* [**password** *password*]

no bind subscriber *sub-name* **modem dhcp** *ctx-name*

Purpose

Binds a port, circuit, channel, or cable modem indirectly to an interface in the specified context according to the IP address within the local (or Remote Authentication Dial-In User Service [RADIUS]) subscriber record for the specified user.

Command Mode

circuit configuration
dot1q pvc configuration
HDLC channel configuration
port configuration

Syntax Description

sub-name	Username and domain name that define the subscriber record to be used. You you configure a custom structured username format, the format of the *sub-name* argument must match (see the **aaa default-domain** and **aaa username-format** commands). Otherwise, the *sub-name* argument must take the default form of *user@domain*.
password *password*	Optional. Password string to be associated with the username. Required if the associated subscriber record or RADIUS record requires a password.

Default

None

Usage Guidelines

Use the **bind subscriber** command to bind a port, circuit, channel, or cable modem indirectly to an interface in the specified context according to the IP address within the local (or RADIUS) subscriber record for the specified user.

This command is only available in the port and HDLC channel configuration modes when the encapsulation has been set to Cisco HDLC or PPP.

Subscriber password strings, if supplied, are not encrypted in the configuration file. A password with embedded spaces can be entered by enclosing the entire password in double quotes.

Note If you enter a new **bind** command for a port, circuit, or channel, the previous binding is removed and any active sessions are dropped. If an existing binding on the port, circuit, or channel is exactly the same as specified in the new **bind** command, the existing binding is not removed.

Use the **no** form of this command to remove the binding.

Examples

The following example sets the encapsulation on a DS-3 port to PPP and then binds the subscriber `george` in the `local` context:

```
[local]RedBack(config)#port ds3 4/1
[local]RedBack(config-port)#encapsulation ppp
[local]RedBack(config-port)#bind subscriber george@local
```

Related Commands

aaa default-domain
aaa username-format
encapsulation

show bindings

show bindings [**all**] [**bound** | **unbound**] [*slot/port* [**hdlc-channel** *chan-name* [*dlci* [**through** *end-dlci*]] | [*vpi* [*vci* [**through** *end-vci*]]]] [**auth** | **bypass** [*bypass-name*] | **dot1q** | **interface** [*if-name*] | **none** | **session** [*peer-name*] | **subscriber** [*sub-name*] | **summary** | **tunnel** [*tunnel-peer*] | **multi-int** | **multi-sub**]

Purpose

Displays the bindings for one or more circuits.

Command Mode

operator exec

Syntax Description

all	Optional. If specified, all circuits are displayed. This option is only valid in the local context.
bound	Optional. Displays only bound circuits.
unbound	Optional. Displays only unbound circuits.
slot/port	Optional. Backplane slot number and port number of an Asynchronous Transfer Mode (ATM) or Frame Relay port.
hdlc-channel *chan-name*	Optional. Specifies the name of the High-level Data Link Control (HDLC) channel. This construct is valid only for channelized DS-3 ports.
dlci	Optional. Data-link connection identifier (DLCI) of a configured Frame Relay permanent virtual circuit (PVC).
through *end-dlci*	Optional. Last DLCI number when specifying a range of circuits.
vpi	Optional. Virtual path identifier (VPI) of a configured ATM PVC.
vci	Optional. Virtual channel identifier (VCI) of a configured ATM PVC. For ATM T1 modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 modules, the range of values is 1 to 4,095; for all ATM Version 2 modules, the range of values is 1 to 65,535.
auth	Optional. Displays only PVCs bound via the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP).
bypass	Optional. Displays only PVCs bound to a bypass.
bypass-name	Optional. Name of a particular bypass for which bindings are displayed.

dot1q	Optional. Displays only 802.1Q to RFC 1483 bridged and 802.1Q to RFC 1490 bridged information.
interface	Optional. Displays only PVCs bound to an interface.
if-name	Optional. Name of a particular interface for which bindings are displayed.
none	Optional. Displays only circuits that have no bindings configured.
session	Optional. Displays only Layer 2 Tunneling Protocol (L2TP) and Layer 2 Forwarding (L2F) session information.
peer-name	Optional. Name of a particular L2TP or L2F peer for which bindings are displayed.
subscriber	Optional. Displays only PVCs bound to subscribers.
sub-name	Optional. Name of a particular subscriber for which bindings are displayed.
summary	Optional. Displays only a summary of bound/unbound PVCs.
tunnel	Optional. Displays only L2TP and L2F tunnel information.
tunnel-peer	Optional. Name of a particular tunnel for which bindings are displayed.
multi-int	Optional. Displays only PVCs configured with the **bind multi** command using the **interface** keyword.
multi-sub	Optional. Displays only PVCs configured with the **bind multi** command using the **subscriber** keyword.

Default

Displays all PVCs that are bound within the current context.

Usage Guidelines

Use the **show bindings** command to display information on configured bindings. Use the optional keywords and arguments to restrict the display to specific permanent virtual circuits of interest.

In the local context, you can use the **all** keyword to display all PVCs, both bound (in any context) and unbound. This keyword is only valid in the local context. In any other context, only PVCs that are bound within the current context are shown

Use the **bound** keyword do display only PVCs that are bound. Use the **unbound** keyword to display binding information only PVCs that are unbound (including PVCs with no configured binding).

Use the *slot/port* argument to restrict the display to include binding information only for PVCs configured on that port.

Use the *dlci* argument to display binding information for a single Frame Relay PVC; use the *dlci* **through** *end-dlci* construct to display a range of Frame Relay PVCs.

Use the *vpi* argument to display binding information only for ATM PVCs with the specified virtual path identifier; use the *vci* argument to display binding information for a specific ATM PVC. Use the *vpi vci* **through** *end-vci* construct to display binding information for a range of ATM PVCs.

Use the **summary** keyword to exclude per-PVC counters from the display, and include only the summary that normally appears at the end of the display .

Use the **auth** keyword to display binding information only for PVCs configured with the **bind authentication** command.

Use the **bypass** keyword to display binding information only for PVCs configured with the **bind bypass** command. Use the *bypass-name* argument to display binding information only for PVCs bound to the specified bypass.

Use the **interface** keyword to display binding information only for PVCs configured with the **bind interface** command. Use the *if-name* argument to display binding information only for PVCs bound to the specified interface.

Use the **session** keyword to display binding information only for PVCs configured with the **bind session** command. Use the *l2tp-peer-name* argument to display binding information only for PVCs that are bound to the specified peer.

Use the **subscriber** keyword to display binding information only for PVCs configured with the **bind subscriber** command. Use the *sub-name* argument to display binding information only for PVCs that are bound to the specified subscriber.

Use the **tunnel** keyword to display binding information only for PVCs configured with the **bind tunnel** command. Use the *l2tp-tunnel-peer* argument to display binding information only for PVCs that are bound to the specified tunnel.

Use the **dot1q** to display binding information only for PVCs configured with the **bind 802.1q** command.

Use the **none** keyword to display only PVCs that have no binding configured.

Use the **multi** keyword to display binding information only for PVCs configured with the **bind multi** command.

Examples

The following example displays binding information for all configured PVCs:

```
[local]RedBack>show bindings all
MON AUG 9 15:21:30 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---   ----    ----        --------- ---------
2/0  Frame 16   BOUND   Routed_1490 subscribr fr1@fr2
2/0  Frame 77   UNBOUND PPP_1490    pap
2/0  Frame 78   UNBOUND PPP_1490
2/0  Frame 79   UNBOUND PPP_1490    chap
2/0  Frame 80   UNBOUND PPP_1490    chap pap
2/0  Frame 100  BOUND   Bridge_1490 interface fr1 [frame]
2/1  Frame 16   BOUND   Bridge_1490 subscribr fr2@fr1
2/1  Frame 55   BOUND   Routed_1490 bypass    by1 [b]
2/1  Frame 56   BOUND   Routed_1490 bypass    by2 [b]
2/1  Frame 58   BOUND   Routed_1490 bypass    by1 [b]
2/1  Frame 60   BOUND   Bridge_1490 bypass    by1 [a]
2/1  Frame 100  BOUND   Bridge_1490 interface fr1 [frame2]
5/0  ATM   1.1  BOUND   Bridge_1483 interface atm50 [atm]
5/0  ATM   2.16 BOUND   PPP         subscribr a@b
```

```
5/0  ATM   2.20 UNBOUND PPP         chap
5/0  ATM   2.22 UNBOUND PPP         chap
5/0  ATM   4.4  BOUND   Bridge_1483 interface atm40 [atm]
5/1  ATM   1.1  BOUND   Bridge_1483 interface atm51 [atm2]
5/1  ATM   1.17 UNBOUND Routed_1483
5/1  ATM   1.18 UNBOUND Bridge_1483
5/1  ATM   1.19 UNBOUND Routed_1483
5/1  ATM   2.16 BOUND   PPP         subscribr b@a
5/1  ATM   4.4  BOUND   Bridge_1483 interface atm41 [atm2]
auth:6    bypass:4   interface:7   subscriber:4
session:0 tunnel:0   dot1q:  0     none:4
bound: 16 unbound:9 total:25
```

In the example above the ‘user[context]’ notation is used in the case of PVCs that are bound using **bind interface** or **bind bypass**. The ‘user@context’ notation is used in cases where the PVC has been bound using a **bind authentication** or **bind subscriber**.

The following example displays all bindings in the current context (b):

```
[b]RedBack>show bindings

MON AUG 9 15:22:02 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---  ----    ----        --------- ---------
2/1  Frame 55  BOUND Routed_1490    bypass    by1 [b]
2/1  Frame 56  BOUND Routed_1490    bypass    by2 [b]
2/1  Frame 58  BOUND Routed_1490    bypass    by1 [b]
5/0  ATM   2.16BOUND PPP subscribr              a@b
```

The following example displays binding information for all PVCs configured with the **bind interface** command on port 5/1:

```
[local]RedBack>show bindings 5/1 interface

MON AUG 9 15:22:23 1999
5/1 ATM 1.1 BOUND Bridge_1483 interface atm51 [atm2]
5/1 ATM  4.4 BOUND Bridge_1483 interface atm41 [atm2]
```

The following example displays all PVCs that do not have a binding configured:

```
[local]RedBack>show bindings none

MON AUG 9 15:22:49 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---  ----    ----        --------- ---------
2/0  Frame 78  UNBOUND  PPP_1490
5/1  ATM  1.17 UNBOUND  Routed_1483
5/1  ATM  1.18 UNBOUND  Bridge_1483
5/1  ATM  1.19 UNBOUND  Routed_1483
```

The following example displays all PVCs which are configured using **bind authentication** that are not yet unbound:

```
[local]RedBack>show bindings unbound auth

MON AUG 9 15:25:48 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---  ----    ----        --------- ---------
2/0  Frame 77   UNBOUND  PPP_1490 pap
2/0  Frame 79   UNBOUND  PPP_1490 chap
2/0  Frame 80   UNBOUND  PPP_1490 chap pap
5/0  ATM  2.20 UNBOUND  PPP chap
5/0  ATM  2.22 UNBOUND  PPP chap
```

The following example displays all bindings for ATM PVC `1:1` on port `5/1`:

```
[local]RedBack>show bindings 5/1 1 1

MON AUG 9 15:26:56 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---  ----    ----        --------- ---------
5/1  ATM  1.2  BOUND    Bridge_1483 interface atm51 [atm2]
```

The following example displays bindings for subscriber `fred` in context `green`:

```
[green]RedBack>show bindings subscriber fred

MON AUG 9 15:27:01 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---  ----    ----        --------- ---------
5/1  ATM  2.16 BOUND    PPP         subscribr fred@green
```

The following example displays bindings for all PVCs configured with the **bind multi** command:

```
[green]RedBack>show bindings multi

MON AUG 9 15:27:01 1999
Port Type  PVC  State   Encaps      Bind Type Bind Name
---- ----  ---  ----    ----        --------- ---------
4/0  ATM 10.10  BOUND   multi       multi     green[local]
```

Related Commands

atm pvc
frame-relay pvc
show atm pvc
show ppp
show pppoe

Part 4

Bridges and Bypasses

Bridging Commands

This chapter describes the commands related to configuring bridging. Use the **bridge** command in context configuration mode to access bridge configuration mode. Bridge commands are used to create and define the behavior of various bridge groups.

For overview information, a description of the tasks used to configure bridging features, and configuration examples, see the “Configuring Bridging” chapter in the *Access Operating System (AOS) Configuration Guide*.

bridge

bridge *bridge-group*

no bridge *bridge-group*

Purpose

Creates or selects a bridge group, and enters bridge configuration mode.

Command Mode

context configuration

Syntax Description

bridge-group	Alphanumeric string providing the name of the new or existing bridge group.

Default

A new bridge group is configured as a bridging-routing bridge.

Usage Guidelines

Use the **bridge** command to create a new bridge group or select an existing bridge group so you can make changes to its configuration. Subscriber Management System (SMS) devices support two types of bridging: bridging-routing and bridging-only. Bridging-routing bridges all protocols except IP, which is routed. Bridging-only bridges all protocols, including IP. A bridge can be Media Access Control (MAC)-based (transparent) or based on the IEEE 802.1D Spanning-Tree Protocol (STP). Multiple bridges can exist in a context.

Only circuits that support a MAC layer can be part of a bridge group. These include Ethernet ports, ATM PVCs with bridged RFC 1483 encapsulation, and Frame Relay PVCs with bridged RFC 1490 encapsulation. PPP-encapsulated circuits cannot be members of a bridge group.

For bridging-routing, first use the **bridge** command to create a bridge group. In interface configuration mode, create an interface for bridging-routing, and then use the **debug ip arp** command to assign the bridge group to the new bridge interface. Separately, create an interface for bridging-only and assign it an IP address. Next, select a subscriber and assign an IP address that corresponds to the bridging-routing interface to the subscriber. Repeat for each subscriber that will be part of the bridge group. In circuit mode, use the **bind subscriber** command to bind each subscriber to a circuit, and then use the **bind interface** command to bind a circuit to the bridging-only interface.

For bridging-only, first use the **bridge** command to create a bridge group. In bridge configuration mode, use the **bridge-only** command to set the bridging type to bridging-only. Select a subscriber and use the **bridge-group** command in subscriber mode to assign the bridge group to the subscriber. Repeat this command for all subscribers that will be part of the bridge group. In circuit mode, use the **bind subscriber** command to bind each subscriber to a circuit.

Use the **no** form of this command to delete an existing bridge group.

Examples

In the following example, a bridge group named `simple_bridge` is created:

```
[local]RedBack(config-ctx)#bridge simple_bridge
[local]RedBack(config-bridge)#
```

Related Commands

bind interface
bind subscriber
debug ip arp—interface configuration mode
bridge-group—subscriber configuration mode
bridge-only
debug bridge span-tree
debug bridge table
show bridge address
show bridge info
show bridge span-tree
show bridge table

bridge-group

bridge-group *name* [**aging-time** *time* | **path-cost** *cost* | **spanning-disabled** | **trans-bpdu** | **access-group** *name* {**in** | **out**}]

no bridge-group *name*

Purpose

Attaches an interface or a subscriber to a previously defined bridge group.

Command Mode

interface configuration
subscriber configuration

Syntax Description

name	Alphanumeric string specifying the previously configured bridge group to which this subscriber is to be attached.
aging-time *time*	Optional. Address age time, in seconds, for the particular circuit that will be bound to this subscriber. This represents the aging of the learned Media Access Control (MAC) addresses. The range is 60 to 1,000,000. The default is 300.
path-cost *cost*	Optional. Path cost to the designated bridge. The total root path cost becomes the cost to the designated bridge plus the cost to root from the designated bridge. The range is 1 to 65,535; the default is 1.
spanning-disabled	Optional. Disables the IEEE 802.1D Spanning-Tree protocol for the particular circuit that will be bound to this subscriber.
trans-bpdu	Optional. Causes the AOS to send spanning-tree bridge protocol data units (BPDUs) in transparent BPDU mode; that is, encapsulated within an 802.3 header using the Ethernet Logical Link Control (LLC) Subnetwork Access Protocol (SNAP) value. By default, spanning-tree BPDUs are encapsulated as specified in RFC 1483 and RFC 1490 with their own LLC SNAP values.
access-group *name*	Optional. Name of a bridge access control list to be attached to the subscriber's circuit. For inbound access control lists (**in** keyword), the packet is filtered by applying the access control list upon receipt from the subscriber's circuit. For outbound access lists (**out** keyword), the packet is filtered prior to transmission by applying the access control list associated with the subscriber's circuit.
in	Applies the access control list to packets received by the subscriber's circuit.
out	Applies the access control list to packets sent by the subscriber's circuit.

Default

The aging time is 300 seconds, the path cost is 1 unit, and the Spanning-Tree Protocol is enabled.

Usage Guidelines

Use the **bridge-group** command in interface configuration mode to attach a bridge group to an interface. Use this command in subscriber configuration mode to attach a bridge group to a subscriber record.

Use the **no** form of this command to disassociate the indicated bridge group from the interface or subscriber record.

Examples

The following example attaches the bridge group `redback-customers` to interface `enet1`:

```
[local]RedBack(config-ctx)#bridge redback-customers
[local]RedBack(config-bridge)#exit
[local]RedBack(config-ctx)#subscriber name thomas
[local]RedBack(config-sub)#bridge-group redback-customers
```

Related Commands

bridge access-list
debug bridge table
show bridge access-list

bridge-only

bridge-only

no bridge-only

Purpose

Bridges all packets, including IP, in a bridge group.

Command Mode

bridge configuration

Syntax Description

This command has no keywords or arguments.

Default

If this command is not used, IP packets are routed, not bridged.

Usage Guidelines

Use the **bridge-only** command to bridge IP packets, instead of routing them, on bridged interfaces.

Use the **no** form of this command to route IP packets and bridge all others on a given interface. IP packets addressed to an interface configured within a context are accepted and processed according to the rules for IP hosts.

See the **bridge** command description for additional information.

Examples

The following example configures all packets, including IP, to be bridged for the bridge named `redback-customers`:

```
[local]RedBack(config-ctx)#bridge redback-customers
[local]RedBack(config-bridge)#bridge-only
```

Related Commands

bridge
debug bridge span-tree
debug bridge table
show bridge address

show bridge info
show bridge span-tree
show bridge table

bridge station-move verbose

bridge station-move verbose

no bridge station-move verbose

Purpose

Enables the logging of bridge station moves detected by the system.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

Bridge station moves are not logged.

Usage Guidelines

Use the **bridge station-move verbose** command to enable the logging of station moves detected by the system. A large number of station move messages could indicate a problem in the network configuration. This command applies to all bridge groups on the system.

Caution Enabling this command could result in a large number of messages.

Use the **no** form of this command to disable bridge station move messages.

Examples

The following example enables the logging of bridge station moves on the system:

```
[local]RedBack(config)#bridge station-move verbose
```

Related Commands

bridge
debug bridge span-tree
debug bridge table

clear bridge table

clear bridge table *bridge-group context*

Purpose

Removes the forwarding table entries for the specified bridge group.

Command Mode

administrator exec

Syntax Description

bridge-group	Name of the bridge group to be cleared.
context	Name of the context in which the bridge group is defined.

Default

None

Usage Guidelines

Use the **clear bridge table** command to remove the forwarding table entries for the specified bridge group in the specified context.

Examples

The following example clears the bridge table for a bridge group named `workgroup` in the `local` context:

```
[local]RedBack#clear bridge table workgroup local
```

Related Commands

show bridge info
show bridge table

debug bridge span-tree

debug bridge span-tree {**all** | **config-bpdu** | **states** | **tcn-bpdu** | **timers**}

no debug bridge span-tree {**all** | **config-bpdu** | **states** | **tcn-bpdu** | **timers**}

Purpose

Prints debugging information pertaining to the Spanning-Tree Protocol (STP).

Command Mode

administrator exec

Syntax Description

all	Enables debugging of the entire spanning-tree.
config-bpdu	Enables debugging of spanning-tree configuration bridge protocol data units (BPDUs).
states	Enables debugging of spanning-tree state transitions.
tcn-bpdu	Enables debugging of spanning-tree topology change notification (TCN) BPDUs.
timers	Enables debugging of spanning-tree timers.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug bridge span-tree** command to enable various types of spanning-tree-related debugging.

Caution Debugging can severely affect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging of spanning-tree related protocol events.

Examples

The following command enables debugging of configuration BPDUs:

```
[local]RedBack#debug bridge span-tree config-bpdu
```

Related Commands

bridge
show bridge span-tree
show debugging

debug bridge table

debug bridge table

no debug bridge table

Purpose

Prints debugging information when entries are added to or removed from a bridge forwarding table.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug bridge table** command to enable debugging related to the addition and removal of items from the bridge forwarding table.

Caution Debugging can severely affect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging of bridge table updates.

Examples

The following example enables debugging of updates to bridge forwarding tables:

```
[local]RedBack#debug bridge table
```

Related Commands

bridge
show debugging

forward-time

forward-time *forward-delay*

default forward-time

Purpose

Configures the IEEE 802.1D Spanning-Tree Protocol (STP) forwarding delay time.

Command Mode

bridge configuration

Syntax Description

forward-delay	Forwarding delay time in seconds. The range of values is 1 to 30; the default is 10.

Default

The forwarding delay time is 10 seconds.

Usage Guidelines

Use the **forward-time** command to configure the IEEE 802.1D STP forwarding delay time. The forwarding delay time is the time that the bridge stays in an intermediate state before changing a port from the blocking state, to the listening state, to the learning state, and finally, to the forwarding state.

Use the **default** form of this command to return the forwarding delay time to 10 seconds.

Examples

The following example sets the forwarding delay time to 8 seconds:

```
[local]RedBack(config-bridge)#forward-time 8
```

Related Commands

bridge
debug bridge span-tree
debug bridge table
show bridge address

show bridge info
show bridge span-tree
show bridge table

hello-time

hello-time *hello-time*

default hello-time

Purpose

Configures the IEEE 802.1D Spanning-Tree Protocol (STP) spanning-tree hello time.

Command Mode

bridge configuration

Syntax Description

hello-time	Spanning-tree hello time in seconds. The range of values is 1 to 10; the default is 2.

Default

The hello time is 2 seconds.

Usage Guidelines

Use the **hello-time** command to configure the IEEE 802.1D STP hello time. The hello time is the time between generation of configuration messages by the bridge root.

Use the **default** form of this command to return the hello time to 2 seconds.

Examples

The following example sets the spanning-tree hello time to 9 seconds:

```
[local]RedBack(config-bridge)#hello-time 9
```

Related Commands

bridge
debug bridge span-tree
debug bridge table
show bridge address
show bridge info
show bridge span-tree
show bridge table

max-age

max-age *max-age*

default max-age

Purpose

Configures the IEEE 802.1D Spanning-Tree Protocol (STP) maximum age time.

Command Mode

bridge configuration

Syntax Description

max-age	Spanning-tree maximum age time in seconds. The range of values is 6 to 40; the default is 20.

Default

The default spanning-tree maximum age time is 20 seconds.

Usage Guidelines

Use the **max-age** command to configure the IEEE 802.1D STP maximum age time. If a new configuration message is not received from the root in the time specified, the existing message is deleted.

Use the **default** form of this command to return the maximum age time to 20 seconds.

Examples

The following example sets the spanning-tree maximum age time to 16 seconds:

```
[local]RedBack(config-bridge)#max-age 16
```

Related Commands

bridge
debug bridge span-tree
debug bridge table
show bridge address
show bridge info
show bridge span-tree
show bridge table

priority

priority *priority*

default priority

Purpose

Configures the bridge priority.

Command Mode

bridge configuration

Syntax Description

priority	Priority of the bridge. The range of values is 0 to 65,535; the default is 32,768. This value can also be entered as a hexadecimal number, as long as the hex number is preceded by 0x; see the “Examples” section.

Default

The default priority is 32768.

Usage Guidelines

Use the **priority** command to configure the most-significant 16 bits of a 64-bit bridge identifier. The other 48 bits represent the bridge’s Media Access Control (MAC) address. The lower the priority, the greater the probability that a node becomes the root.

Use the **default** form of this command to return the priority to the value of 32,768.

Examples

The following example sets the bridge priority to `2000` (hexadecimal):

```
[local]RedBack(config-bridge)#priority 0x2000
```

The following example sets the bridge priority to `32000` (decimal):

```
[local]RedBack(config-bridge)#priority 32000
```

Related Commands

bridge
debug bridge span-tree
debug bridge table
show bridge address
show bridge info
show bridge span-tree
show bridge table

protocol

protocol ieee

default protocol

Purpose

Selects the IEEE 802.1D Spanning-Tree Protocol (STP).

Command Mode

bridge configuration

Syntax Description

ieee	Selects the IEEE 802.1D Spanning-Tree Protocol.

Default

The protocol is IEEE 802.1D Spanning-Tree Protocol.

Usage Guidelines

Use the **protocol** command to select IEEE 802.1D Spanning-Tree Protocol as the bridge protocol to use. Currently, IEEE 802.1D Spanning-Tree Protocol is the only bridge protocol supported by Subscriber Management System (SMS) devices. Since the default specifies this protocol also, it is not necessary to enter this command into the configuration.

To disable the IEEE 802.1D Spanning-Tree Protocol, provide the **spanning-disabled** keyword to the **bridge-group** command in either interface configuration mode or subscriber configuration mode.

The **default** form of this command has the same effect as the **protocol** command itself, which is to select IEEE 802.1D Spanning-Tree Protocol as the bridge protocol.

Examples

The following example selects the IEEE 802.1D Spanning-Tree Protocol:

```
[local]Redback(config-bridge)#protocol ieee
```

Related Commands

bridge
debug ip arp—interface configuration mode
bridge-group—subscriber configuration mode

debug bridge span-tree
debug bridge table
show bridge address
show bridge info
show bridge span-tree
show bridge table

show bridge address

show bridge address *mac-address*

Purpose

Displays information about a specific host, identified by a Media Access Control (MAC) address.

Command Mode

administrator exec

Syntax Description

mac-address	MAC address of the host.

Default

None

Usage Guidelines

Use the **show bridge address** command to display information about a host. Since bridge forwarding tables can be very long, this command offers a way to display information about a specific host when you know the corresponding MAC address. This is a useful tool when trying to determine connectivity in a bridged environment.

Examples

The following example causes the Access Operating System (AOS) to search the bridge forwarding table for the `local` context to find the specified MAC address, and display information for the corresponding host:

```
[local]RedBack#show bridge address 00:10:67:00:04:29

(Context = local, Bridge Group = workgroup)
Slot/Port  VPI VCI    Address           Age Time (sec)
---------  --- -----  ----------------- --------------
5/1        0   101    00:10:67:00:04:29 +213
```

Related Commands

bridge

show bridge info

show bridge info [**all**]

Purpose

Displays a list of bridge groups configured in the current context.

Command Mode

administrator exec

Syntax Description

all	Optional. Displays bridge groups in all contexts. This keyword is only available to administrators in the local context.

Default

None

Usage Guidelines

Use the **show bridge info** command to display a list of bridge groups. Used without any optional keywords, this command displays a list of the bridge groups in the current context only. Used with the optional **all** keyword, this command displays a list of the bridge groups in all contexts. The **all** keyword is ignored if the operator is not authenticated to the local context.

Examples

The following example uses the **show bridge info** command to display a list of bridge groups in the local context:

```
[local]RedBack#show bridge info

Context    Bridge Group  Circuits  Priority
-------    ------------  --------  --------
local      workgroup     0         32768
local      ipx-folks     3         12288
```

Related Commands

bridge
show bridge table

show bridge span-tree

show bridge span-tree {**detail** | **states**} [*bridge-group*]

Purpose

Shows various spanning-tree information for bridge groups in the current context.

Command Mode

administrator exec

Syntax Description

detail	Specifies a detailed listing of spanning-tree information.
states	Specifies information relating to states of the spanning-tree circuits.
bridge-group	Optional. Name of a configured bridge-group.

Default

None

Usage Guidelines

Use the **show bridge span-tree** command to display spanning-tree information for a specific bridge group or all bridge groups in the current context.

Examples

The following example uses the **show bridge span-tree** command with the **states** keyword to display spanning-tree circuit state information:

```
[local]RedBack#show bridge span-tree states

BRIDGE GROUP = workgroup:
(Designated Root = 1000.0080.5000.8707)
Slot/           CCT        Path Root    Designated       Desig Desig       Addr
Port  VPI VCI   ID   State Cost Cost      Bridge          CCT  Cost  Flags Cnt
----- --- ---- ----- ----- ---- ---- ------------------ ----- ----- ----  ----
5/1  0    103  000a  BLK   1    1    2000.0010.6700.138e 0004  1     D     0
5/1  0    101  0008* FWD   1    1    1000.0080.5000.8707 0002  0     D     1
5/0  0    105  0006  FWD   1    1    3000.0010.6700.138f 0006  1     D     0
```

```
[local]RedBack#show bridge span-tree detail

BRIDGE GROUP = workgroup:
  Bridge Id = 3000.0010.6700.138f Designated Root Addr = 1000.0080.5000.8707
  Root Circuit = [ME]                Root Path Cost = 0
  Max Age = 20                       Hello Time = 2
  Fwd Delay = 15                     Bridge Max Age = 20
  Bridge Hello Time = 2              Bridge Fwd Delay = 15
  Topology Change Time = 35          Hold Time = 1
  Topology Change Detected = FALSE   Topology Change = FALSE
  BPDUs rcvd = 0                     BPDUs sent = 0
  TCNs rcvd = 0                      TCNs sent = 0
  BPDU max age rejects = 0           BPDU hello time rejects = 0
  BPDU fwd delay rejects = 0         Total BPDUs/TCNs rejected = 0
  Total Circuits = 0                 Total addresses = 0

  Forwarding Statistics:
    Pkts sent = 0                    Pkts rcvd = 38092
    Pkts dropped = 0                 Station moves = 0
    Floods = 0                       BCAST/MCAST destinations = 0
    Encap failures = 0               Msg ring post failures = 0
```

Table 21-1 provides a description of the display fields in the **show bridge span-tree detail** command output.

Table 21-1 Field Descriptions for show bridge span-tree detail Command

Display Field	Description
BRIDGE GROUP	Name of the bridge group
Bridge Id	Identification of the bridge, a combination of the bridge priority and the bridge Media Access Control (MAC) address
Designated Root Addr	MAC address of the spanning-tree root node
Root Circuit	Handle of the root node of the spanning-tree mesh
Root Path Cost	Cost of this spanning-tree path (used to resolve the path in a looped or mesh environment)
Max Age	Maximum acceptable age of received bridge protocol data units (BPDUs)
Hello Time	Maximum allowable time between reception of bridge Hello PDUs
Fwd Delay	IEEE 802.1 timer
Bridge Max Age	IEEE 802.1 timer
Bridge Hello Time	IEEE 802.1 timer
Bridge Fwd Delay	IEEE 802.1 timer
Topology Change Time	Sum of the bridge Max Age and Bridge Forward Delay parameters
Hold Time	Always 1 second, according to IEEE 802.1D

Table 21-1 Field Descriptions for show bridge span-tree detail Command

Display Field	Description
Topology Change Detected	Specifies whether a spanning-tree topology change has been detected
Topology Change	Specifies whether a state change has been detected
BPDUs rcvd	Number of BPDUs received by this spanning-tree node
BPDUs sent	Number of BPDUs sent by this spanning-tree node
TCNs rcvd	Number of topology change notification (TCN) BPDUs received by this spanning-tree node
TCNs sent	Number of TCN BPDUs sent by this spanning-tree node
BPDU max age rejects	Number of BPDUs received that have expired
BPDU hello time rejects	Number of BPDUs rejected due to exceeding the Hello Time
BPDU fwd delay rejects	Number of BPDUs rejected due to an invalid Fwd Delay value
Total PBDUs/TCNs rejected	Total number of rejected BPDUs
Total Circuits	Total number of bridge interfaces in the bridge group
Total addresses	Total number of forwarding table entries
Pkts sent	Number of packets forwarded by this node
Pkts rcvd	Number of packets received by this node
Pkts dropped	Number of packets dropped by this node
Station moves	Number of MAC addresses that have been detected on multiple interfaces
Floods	Number of unicast packets flooded out interfaces
BCAST/MCAST destinations	Number of packets sent out all bridge group interfaces
Encap failures	Number of datagram encapsulation failures within the bridged group
Msg ring post failures	Number of datagrams/messages that failed to post to an internal ring

Related Commands

bridge

show bridge table

show bridge table [*bridge-group*]

Purpose

Displays the Media Access Control (MAC) forwarding table for a specific bridge or all bridges in the current context.

Command Mode

administrator exec

Syntax Description

bridge-group	Optional. Name of a configured bridge group.

Default

The forwarding table of all bridge groups in the current context is displayed.

Usage Guidelines

Use the **show bridge table** command to display the bridge forwarding table for a specific bridge group or all bridge groups in the current context.

Examples

The following example displays the bridge forwarding table for the local context:

```
[local]RedBack#show bridge table

(Context = local, Bridge Group = workgroup)
Slot/Port  VPI  VCI    Address            Age Time (sec)
---------  ---  -----  -----------------  --------------
5/1        0    101    00:10:67:00:04:14  +87
5/1        0    101    00:10:67:00:04:29  +213
5/1        0    101    00:10:67:00:05:18  +230
5/1        0    103    00:10:67:00:04:71  +290
```

Related Commands

bridge
debug ip arp—interface configuration mode
bridge-group—subscriber configuration mode

Bypass Commands

This chapter includes the commands related to configuring bypasses. Use the **bypass** context configuration command to create a bypass and access bypass configuration mode.

For overview information, a description of the tasks used to configure bypass features, and configuration examples, see the “Configuring Bypasses” chapter in the *Access Operating System (AOS) Configuration Guide*.

bypass

bypass *bypass-name*

no bypass *bypass-name*

Purpose

Creates a new bypass and enters bypass configuration mode where you can configure the new bypass or make changes to the configuration of an existing one.

Command Mode

context configuration

Syntax Description

bypass-name	Alphanumeric string.

Default

None

Usage Guidelines

Use the **bypass** command to create a new bypass and enter bypass configuration mode. Bypasses allow a network administrator to bind two circuits, channels, or ports together without protocol translation. The Subscriber Management System (SMS) device simply relays link-layer frames between the two circuits without the interpretation of high-layer protocols.

Once you have created the bypass, use the **bind bypass** command in either port, High-Level Data Link Control (HDLC) channel, or circuit configuration mode to bind two ports or circuits together.

Deleting a bypass removes the binding of any circuit bound to that bypass.

Use the **no** form of this command to delete the bypass.

Examples

The following example creates a bypass called `bypass10_20`:

```
[local]Redback(config-ctx)#bypass bypass10_20
[local]Redback(config-bypass)
```

Related Commands

bind bypass
show bypass

description

description *text*

no description

Purpose

Assigns a text description to a bypass.

Command Mode

bypass configuration

Syntax Description

text	Textual description of a bypass. Can be any alphanumeric string, including spaces, that is not longer than one line. The text will not wrap to the next line.

Default

None

Usage Guidelines

Use the **description** command to associate descriptive information with a bypass. The textual description appears in the output of the **show bypass** and **show configuration** commands. To change a description, create a new one, and it overwrites the existing one.

Use the **no** form of this command to remove any previously defined description.

Examples

The following example uses the **description** command to note that the bypass named `switcher` is provisioned for `ma-n-pa.net`:

```
[local]RedBack(config)#bypass switcher
[local]RedBack(config-bypass)#description For ma-n-pa.net
```

Related Commands

show bypass
show configuration

show bypass

show bypass [*bypass-name*]

Purpose

Displays binding information for one or all bypasses configured for the current context.

Command Mode

operator exec

Syntax Description

bypass-name	Optional. Name of a configured bypass for which you want information displayed.

Default

Displays information for all bypasses in the current context.

Usage Guidelines

Use the **show bypass** command to display information about one or all bypasses in the current context. A bypass can have one of three binding states: Unbound (no bindings), Partial (one binding), and Bound (both bindings). The state of each bypass in the current context is shown in the output of this command, along with the port and circuit bindings and the description of the bypass as configured with the **description** command.

Examples

The following example shows sample output from the **show bypass** command:

```
[local]RedBack>show bypass

Bypass Name  Port  Circuit  Port  Circuit  State    Description
-----------  ----  -------  ----  -------  -------  ------------------
super2       5/1   2.55     4/0   1.20     Bound    created 10/12 by al
atm2_bypass  4/0   3.333                   Partial  atm bridged 1483
bypass3                                    Unbound  testing
```

Related Commands

bind bypass
bypass
description
show bindings

Part 5

Point-to-Point Protocol

PPP and PPPoE Commands

This chapter describes the commands used to configure Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure PPP and PPPoE features, and configuration examples, see the "Configuring PPP and PPPoE" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug ppp

debug ppp {**all** | **auto** | **authentication** | **fsm-calls** | **fsm-state** | **ipcp** | **lcp** | **multilink** | **ccp** | **negotiation** | **packets** | **phase** | **filter** {**handle** *value* | **pvc** *slot/port* [*vpi vci* | *dlci*] | **subscriber** *name*}}

no debug ppp {**all** | **authentication** | **fsm-calls** | **fsm-state** | **ipcp** | **lcp** | **multilink** | **negotiation** | **packets** | **phase** | **filter**}

Purpose

Enables the logging of Point-to-Point Protocol (PPP) debugging messages.

Command Mode

administrator exec

Syntax Description

all	Enables debugging of all the following items.
auto	Specifies that the encapsulation for the ppp auto circuit is to be logged any time its encapsulation changes; that is, when the Subscriber Management System (SMS) device automatically detects the encapsulation, and when the encapsulation is reset back to ppp auto for this circuit.
authentication	Enables Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) authentication debugging.
fsm-calls	Enables finite state machine (FSM) calls debugging.
fsm-state	Enables FSM state-change debugging.
ipcp	Enables IP Control Protocol (IPCP) debugging.
lcp	Enables Link Control Protocol (LCP) debugging.
multilink	Enables multilink PPP (MP) debugging.
ccp	Enables PPP compression debugging.
negotiation	Enables PPP negotiation debugging.
packets	Enables PPP packet level debugging.
phase	Enables PPP phase debugging.
filter	Enables debugging filter.
handle *value*	Displays PPP log messages for a specific circuit handle.
pvc *slot/port*	Displays PPP log messages for a specific permanent virtual circuit (PVC).

vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI) of the ATM PVC. The range of VPI values is 0 to 255. For ATM T1 modules, the range of VCI values is 1 to 1,023; for ATM DS-3 Version 1 modules, the range is 1 to 2,047; for ATM OC-3 Version 1 modules, the range is 1 to 4,095; for all ATM Version 2 modules, the range is 1 to 65,535.
dlci	Data-link connection identifier (DLCI) of the Frame-Relay PVC.
subscriber *name*	Name of the subscriber for whose PVC you want PPP log messages displayed.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ppp** command to enable various types of PPP debugging messages.

By default, the debug output is sent to the log. If you want to have debug output sent to the console, enter the **logging console** global configuration command. If you are connected via Telnet, enter the **terminal monitor** operator exec command.

Use the **filter** keyword to restrict debugging to a specific circuit handle, PVC, or subscriber.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable debugging of PPP.

Examples

The following example shows PPP negotiation debugging information:

```
[local]RedBack#debug ppp negotiation

12:09:24 29Dec1977: %PPP-7-SENT_PKT: fsm_sdata: 0x2900003a: P-8021: sent id 87, code 2
12:09:27 29Dec1977: %PPP-7-RCV_PKT: fsm_rconfreq: 0x2900003a: P-8021: sent id 87
12:09:27 29Dec1977: %PPP-7-RCV_CI: ipcp_reqci: 0x2900003a: P-8021: rcvd ADDR.
12:09:27 29Dec1977: %PPP-7-CI_RET: ipcp_reqci: 0x2900003a: P-8021: Returning CONFACK.
12:09:27 29Dec1977: %PPP-7-SENT_PKT: fsm_sdata: 0x2900003a: P-8021: sent id 87, code 2
12:09:27 29Dec1977: %PPP-7-SENT_PKT: fsm_sdata: 0x2900003a: P-8021: sent id 160, code 1
12:09:29 29Dec1977: %PPP-7-SENT_PKT: fsm_sconfreq: 0x2900003a: P-8021: sent id 160,
code 0
12:09:29 29Dec1977: %PPP-7-RCV_PKT: fsm_sconfack 0x2900003a: P-8021: rcvd id 160
```

The following example enables PPP debugging information related to a specific permanent PVC and DLCI:

```
[local]RedBack#debug ppp filter pvc 4/0 21
```

The following example enables MP debugging and shows sample output when four links in two multilink bundles are brought down and then back up again:

```
[local]RedBack#debug ppp multilink

20:39:00 7Mar2000: %PPP-7-MP_LNK_DN: 28000021: Bundle ID 1, Link count 1
20:39:00 7Mar2000: %PPP-7-MP_LNK_DN: 29000021: Bundle ID 2, Link count 1
20:39:01 7Mar2000: %PPP-7-MP_LNK_DN: 28000020: Bundle ID 1, Link count 0
20:39:02 7Mar2000: %PPP-7-MP_LNK_DN: 29000020: Bundle ID 2, Link count 0
20:39:03 7Mar2000: %PPP-7-MP_LNK_UP: 28000021: Bundle ID 3, Link count 1
20:39:03 7Mar2000: %PPP-7-MP_LNK_UP: 29000021: Bundle ID 4, Link count 1
20:39:05 7Mar2000: %PPP-7-MP_LNK_UP: 28000020: Bundle ID 3, Link count 2
20:39:05 7Mar2000: %PPP-7-MP_LNK_UP: 29000020: Bundle ID 4, Link count 2
```

Related Commands

logging console
ppp keepalive
ppp mtu
ppp passive
show debugging
terminal monitor

debug pppoe

debug pppoe {**all** | **discovery** | **vcct**}

no debug pppoe

Purpose

Enables the logging of Point-to-Point Protocol over Ethernet (PPPoE) debugging messages.

Command Mode

administrator exec

Syntax Description

all	Enables both PPPoE discovery protocol and PPPoE virtual circuit debugging.
discovery	Enables PPPoE discovery protocol debugging.
vcct	Enables PPPoE virtual circuit debugging.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug pppoe** command to enable various types of PPPoE debugging messages.

By default, the debug output is sent to the log. If you want to have debug output sent to the console, enter the **logging console** global configuration command. If you are connected via Telnet, enter the **terminal monitor** operator exec command.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables all PPPoE debugging:

```
[local]RedBack#debug pppoe all
```

Related Commands

domain—context configuration mode
logging console
pppoe motm
pppoe services
pppoe url
show debugging
terminal monitor

debug ip ppp-proxy-arp

debug ip ppp-proxy-arp

no debug ip ppp-proxy-arp

Purpose

Enables the logging of Point-to-Point Protocol (PPP) proxy Address Resolution Protocol (ARP) debugging messages.

Command Mode

administrator exec

Syntax Description

This command contains no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip ppp-proxy-arp** command to enable the logging of debugging messages related to PPP proxy ARP.

By default, the debug output is sent to the log. If you want to have debug output sent to the console, enter the **logging console** global configuration command. If you are connected via Telnet, enter the **terminal monitor** operator exec command.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example shows enabling PPP proxy ARP debugging:

```
[local]RedBack#debug ip ppp-proxy-arp
```

Related Commands

logging console
show debugging
terminal monitor

interface

interface *interface-name* [**loopback**] [**ppp-default**]

no interface *interface-name*

Purpose

Creates a new interface or allows changes to an existing interface, and enters interface configuration mode.

Command Mode

context configuration

Syntax Description

interface-name	Alphanumeric string for the name of the interface.
loopback	Specifies that the interface is a loopback interface.
ppp-default	Creates a default Point-to-Point Protocol (PPP) interface that is to act as a fall back for incoming PPP connections.

Default

None

Usage Guidelines

Use the **interface** command to create a new interface, specify that it is to be used as a default PPP interface, and enter interface configuration mode. Ordinarily, PPP sessions that attempt to come up and cannot bind to a valid interface simply fail. A PPP default interface acts as a fall back for those incoming PPP connections. If a PPP session is established, and there is no valid interface to which it can bind, the session binds to the default interface.

The default interface is a virtual interface; there is no actual outgoing circuit. Therefore, a proxy is necessary. One or more interfaces that are not the default interface are set up as proxies using the **ip ppp-proxy-arp** command. The outgoing circuits from these proxies can then be used to handle the traffic on the virtual default interface.

You must assign an IP address to the PPP default interface, but you cannot enter a subnet mask. The netmask is always assumed to be 255.255.255.255. You cannot configure secondary IP addresses for a PPP default interface. You can only use the following interface configuration commands to configure a PPP default interface: **description**, **ip address**, **ip access-group**, **ip igmp**, and **ip mtu**.

Use the **no** form of this command to delete the interface.

Caution Deleting an interface removes all bindings to the interface. If more than one circuit is bound to an interface, the Subscriber Management System (SMS) device does not send Routing Information Protocol (RIP) updates on any of those circuits.

Note This command is also described in Chapter 7, “Interface Commands.”

Examples

The following example configures the interface called `ppp-connections` as a PPP default interface:

```
[local]RedBack(config-ctx)#interface ppp-connections ppp-default
```

Related Commands

bind interface
ip ppp-proxy-arp

ip ppp-proxy-arp

ip ppp-proxy-arp

no ip ppp-proxy-arp

Purpose

Enables proxy Address Resolution Protocol (ARP) functionality on behalf of Point-to-Point Protocol (PPP) circuits that are bound to a PPP default interface.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

Proxy ARP is not enabled.

Usage Guidelines

Use the **ip ppp-proxy-arp** command to enable proxy ARP functionality for PPP default interfaces.

Ordinarily, PPP sessions that attempt to come up and cannot bind to a valid interface simply fail. A PPP default interface will act as a fall back for those incoming PPP connections. If a PPP session is established, and there is no valid interface to which it can bind, the session binds to the default interface.

The default interface is a virtual interface; there is no actual outgoing circuit. Therefore, a proxy is necessary. One or more interfaces that are not the default interface are set up as proxies using the **ip ppp-proxy-arp** command. The outgoing circuits from these proxies can then be used to handle the traffic on the virtual default interface.

Use the **no** form of this command to disable proxy ARP functionality.

Examples

The following example sets up an interface as a proxy for the virtual default PPP interface:

```
[local]RedBack(config-ctx)#interface ppp-connections ppp-default
[local]RedBack(config-if)#ip address 10.1.1.1
[local]RedBack(config-if)#exit
[local]RedBack(config-ctx)#interface proxy1
[local]RedBack(config-if)#ip ppp-proxy-arp
```

Related Commands

bind interface
interface

port-limit

port-limit *max-sessions*

no port-limit

Purpose

Specifies the number of links that a subscriber is authorized to consume simultaneously.

Command Mode

subscriber configuration

Syntax Description

max-sessions	Number of links a subscriber is permitted to consume simultaneously. The range of values is 1 to 255.

Default

There is no limit to the number of links a subscriber may consume.

Usage Guidelines

Use the **port-limit** command for the default subscriber record or for individual subscriber records. Setting a limit on the number of links that a subscriber can consume is useful in preventing dialup or integrated services digital network (ISDN) users from consuming more than their allocated number of links. It can also prevent a single user's account from being accessed by multiple users at the same time.

To set the port limit remotely via RADIUS, use the Port-Limit RADIUS attribute described in the "RADIUS Attributes" appendix of the *Access Operating System (AOS) Configuration Guide*.

Use the **no** form of this command to remove a port limit.

Note This command description also appears in Chapter 8, "Subscriber Commands."

Examples

The following example establishes that subscriber `joe` can only use two links at a time:

```
[local]RedBack(config)#subscriber joe
[local]RedBack(config-sub)#port-limit 2
```

Related Commands

ppp multilink enable
show subscribers

ppp compression

ppp compression

no ppp compression

Purpose

Enables Point-to-Point Protocol (PPP) compression in the subscriber's sessions.

Command Mode

subscriber configuration

Syntax Description

This command has no keywords or arguments.

Default

PPP compression is disabled.

Usage Guidelines

Use the **ppp compression** command to enable PPP compression in the subscriber's sessions, compressing the PPP payload. PPP compression can compress the entire IP datagram (not just the IP header), and can do it without examining the layer 3 headers. Compression improves the effective throughput of the underlying data streams.

SMS devices support two types of PPP compression, Microsoft Point-to-Point Compression (MPPC) and Stac Lempel-Ziv-Stac (Stac LZS). In either case, PPP compression must be negotiated with the peer. MPPC compression is negotiated first, followed by Stac LZS if necessary.

Use the **no** form of this command to disable PPP compression.

Examples

The following example enables PPP compression for a subscriber named `atlas1`:

```
[local]Redback(config)#subscriber name atlas1
[local]Redback(config-sub)#ppp compression
```

Related Commands

show ppp compression

ppp keepalive

ppp keepalive *period*

{**no** | **default**} **ppp keepalive**

Purpose

Enables the sending of Point-to-Point Protocol (PPP) keepalive packets for active PPP sessions.

Command Mode

context configuration

Syntax Description

period	Time in minutes between successive keepalive packets. The range of values is 5 to 14,400. The default is that keepalive packets are not sent, except for circuits using PPP over Ethernet (PPPoE), where the default is 30 minutes.

Default

Keepalive packets are not sent, except in the case of circuits using PPPoE, where the period between the sending of keepalive packets is 30 minutes.

Usage Guidelines

Use the **ppp keepalive** command to enable the sending of PPP keepalive packets for active PPP sessions. When enabled, keepalive packets are sent over every active PPP session in the context and are retransmitted every time interval designated by the *period* argument.

If no response is received after sending a PPP keepalive, the Subscriber Management System (SMS) device enters fast-keepalive mode in which three keepalive packets are transmitted within 10 seconds of each other. If all three transmissions go unanswered, the PPP session is torn down.

Use the **no** or the **default** form of this command to disable the sending of PPP keepalive packets.

Examples

The following example causes PPP keepalives to be transmitted every 10 minutes:

```
[local]RedBack(config-ctx)#ppp keepalive 10
```

Related Commands

debug ppp
ppp mtu
show ppp

ppp mtu

ppp mtu *mtu*

no ppp mtu

Purpose

Sets the maximum transmission unit (MTU) used by Point-to-Point Protocol (PPP) for a subscriber's circuit.

Command Mode

subscriber configuration

Syntax Description

mtu	Maximum transmission unit in bytes. The range of values is 128 to 16,384; the default is 1,500.

Default

The MTU is 1,500 bytes.

Usage Guidelines

Use the **ppp mtu** command to set the MTU for a subscriber circuit.

Use the **no** form of this command to restore the default MTU to 1,500 bytes.

Examples

The following command sets the PPP MTU to 768 bytes:

```
[local]RedBack(config-sub)#ppp mtu 768
```

Related Commands

subscriber
ip mtu

ppp multilink enable

ppp multilink enable

no ppp multilink enable

Purpose

Enables the negotiation of multilink Point-to-Point Protocol (MP).

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

MP is disabled.

Usage Guidelines

Use the **ppp multilink enable** command to enable the negotiation of MP. This command is entered in global configuration mode because MP negotiation occurs prior to authentication. When MP is enabled, the Subscriber Management System (SMS) device sends the option for endpoint discriminator and maximum received reconstructed unit (MRRU) in all of the initial PPP configuration requests, indicating that MP is supported if the peer agrees. The SMS device also accepts incoming PPP configuration requests containing endpoint discriminator and MRRU information, assuming the values are acceptable. If both sides do not agree to negotiate MP, they use PPP instead.

Note You must enter the **ppp multilink enable** command before the **ppp multilink endpoint-discriminator** and **ppp multilink mrru** commands become available.

Using MP causes two extra Remote Authentication Dial-In User Service (RADIUS) attributes to be placed in each RADIUS accounting packet. See the “RADIUS Attributes” appendix in the *Access Operating System (AOS) Configuration Guide* for details on the Acct-Multi-Session-Id and Acct-Link-Count attributes.

Use the **no** form of this command to disable MP.

Examples

The following example enables MP:

```
[local]RedBack(config)#ppp multilink enable
```

Related Commands

port-limit
ppp multilink endpoint-discriminator
ppp multilink mrru
show ppp

ppp multilink endpoint-discriminator

ppp multilink endpoint-discriminator {**class-1** *text* | **class-2** *ip-address* | **class-3** *mac-address* | **class-5** *text* | **local-ip-address** | **local-mac-address**}

default ppp multilink endpoint-discriminator

Purpose

Configures the class and corresponding value to be used for endpoint discriminator negotiation.

Command Mode

global configuration

Syntax Description

class-1 *text*	Class 1 endpoint discriminator as defined by RFC 1990, *The PPP Multilink Protocol (MP)*—with a locally assigned address. The *text* argument is a string of up to 20 characters.
class-2 *ip-address*	Class 2 endpoint discriminator as defined by RFC 1990—with an IP address. The *ip-address* argument is the specific address you want to use.
class-3 *mac-address*	Class 3 endpoint discriminator as defined by RFC 1990—with an IEEE 802.1 Media Access Control (MAC) address. The *mac-address* argument is a 48-bit address in the form hh:hh:hh:hh:hh:hh where hh is a hexadecimal number.
class-5 *text*	Class 5 endpoint discriminator as defined by RFC 1990—with a public switched network directory number. The *text* argument is a string of up to 15 characters representing an E.164 international telephone directory number.
local-ip-address	Specifies a Class 2 endpoint discriminator that uses the IP address of the management port.
local-mac-address	Specifies a Class 3 endpoint discriminator that uses the MAC address of the management port.

Default

The endpoint discriminator is of Class 3 with a MAC address of the management port of the Subscriber Management System (SMS) device.

Usage Guidelines

Use the **ppp multilink endpoint-discriminator** command to define the endpoint discriminator. The endpoint discriminator is important in identifying peers to the system and distinguishing peers from one another in the system. This identification ensures that the correct links are bundled together in the same multilink bundle.

Note You must enter the **ppp multilink enable** command before the **ppp multilink endpoint-discriminator** command is available.

Use the **default** form of this command to return the endpoint discriminator identification to a Class 3 with the MAC address of the SMS device's management port.

Examples

The following command defines an endpoint discriminator as a Class 2 with the IP address of the management port:

```
[local]RedBack(config)#ppp multilink endpoint-discriminator local-ip-address
```

Related Commands

ppp multilink enable

ppp multilink mrru

ppp multilink mrru *bytes*

default ppp multilink mrru

Purpose

Sets the initial maximum received reconstructed unit (MRRU) for Link Control Protocol (LCP) negotiation.

Command Mode

global configuration

Syntax Description

bytes	Size in bytes of the initial MRRU. The default value is 1,500.

Default

The initial MRRU is set to 1,500 bytes.

Usage Guidelines

Use the **ppp multilink mrru** command to set the initial MRRU for LCP negotiation. The MRRU specifies the maximum size of the information fields of reassembled packets. The system must be able to handle an MRRU of 1,500 bytes, but you can use this command to attempt to negotiate a higher or lower value.

Note You must enter the **ppp multilink enable** command before the **ppp multilink mrru** command is available.

Use the **default** form of the command to return the initial MRRU to 1,500 bytes.

Examples

The following command sets an initial MRRU to `1200`:

```
[local]RedBack(config)#ppp multilink mrru 1200
```

Related Commands

ppp multilink enable
show ppp

ppp our-options

ppp our-options mru initial *initial-mru* **max** *max-mru*

default ppp our-options mru

Purpose

Configures how the Subscriber Management System (SMS) device is to negotiate Link Control Protocol (LCP) option values for the local end of the Point-to-Point Protocol (PPP) session.

Command Mode

global configuration

Syntax Description

mru	Indicates that maximum receive unit (MRU) values follow.
initial *initial-mru*	The MRU value at which negotiation begins. The range of values is 128 to 16,384; the default is 1500 for PPP circuits, and 1492 for PPP over Ethernet (PPPoE) circuits.
max *max-mru*	The maximum MRU value for the local device. The range of values is 128 to 16,384; the default is 16,384.

Default

If you do not use this command, the SMS device uses the default option values. For MRU, that value is 1500.

Usage Guidelines

Use the **ppp our-options** command to establish how the local SMS device is to negotiate LCP option values for the local end of PPP sessions. Currently, the options available are the initial and maximum MRU values. When these values are configured, the SMS device begins negotiation for its MRU at the value of the *initial-mru* argument, and does not exceed the value of the *max-mru* argument. The resulting size guidelines are reflected in all packets sent to the local device by the remote peer.

If, after 10 attempts, an agreement with the peer can not be reached as to a local MRU between the configured initial and maximum values, the local SMS device establishes the PPP session without negotiating the local MRU. In that case, an MRU of 1500 is used.

Use the **default** form of this command to return the LCP options to their default values.

Examples

The following example sets the local initial and maximum MRU values:

```
[local]RedBack(config)#ppp our-options mru initial 1800 max 11000
```

Related Commands

ppp our-options

ppp passive

ppp passive

no ppp passive

Purpose

Enables Point-to-Point Protocol (PPP) oversubscription. This command sets a Subscriber Management System (SMS) device to function in “passive mode,” which means that only active PPP sessions count toward the maximum number of bind authentications.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

Passive mode is disabled.

Usage Guidelines

Use the **ppp passive** command to set the SMS device to function in passive mode. By configuring the system to operate in passive mode, this command increases the number of bind authentications you can have, beyond the number that could actually bind and come up. In passive mode, no PPP structures are allocated unless, or until, a peer initiates a session. Once established, the subscriber is counted as a bind authentication in terms of the maximum subscribers that are allowed. When a peer ends a session, that subscriber is no longer counted and the PPP structures are deallocated.

In the default mode (passive mode disabled), PPP structures are allocated for every **bind authentication** command at the time the circuit is configured. It may not be necessary to use passive mode in circumstances where every bind authentication will be active.

Note With passive mode set, the peers must always initiate their sessions. In other words, the SMS device never initiates sessions, even to reestablish disconnected sessions. This is not the case when PPP passive mode is disabled.

Passive mode does not affect the maximum number of subscribers that can be terminated in a particular context (established by the **aaa max-subscribers** command) or the hard limits allowed by the SMS device.

Use the **no** form of this command to disable passive mode.

Examples

The following example configures the system to operate in PPP passive mode:

```
[local]RedBack(config)#ppp passive
```

The following example disables passive mode operation:

```
[local]RedBack(config)#no ppp passive
```

Related Commands

aaa max-subscribers
bind authentication

ppp peer-options

ppp peer-options mru min *min-mru* **max** *max-mru*

default ppp peer-options mru

Purpose

Configures how the Subscriber Management System (SMS) device is to negotiate Link Control Protocol (LCP) option values for the remote end of the Point-to-Point Protocol (PPP) session.

Command Mode

global configuration

Syntax Description

mru	Indicates that maximum receive unit (MRU) values follow.
min *min-mru*	The minimum MRU value for the remote peer. The range of values is 128 to 16,384; the default is 128.
max *max-mru*	The maximum MRU value for the remote peer. The range of values is 128 to 16,384; the default is 16,384.

Default

No remote peer LCP options are negotiated.

Usage Guidelines

Use the **ppp peer-options** command to establish how the SMS device is to negotiate LCP option values for the remote peer end of PPP sessions. Currently, the options available are the minimum and maximum MRU values. When these values are configured, the SMS device negotiates the remote peer's MRU value to be at least the value specified by the *min-mru* argument, and not greater than the value specified by the *max-mru* argument. The resulting size guidelines are reflected in all packets that the SMS device sends to the remote peer.

If, after 10 attempts, the SMS device has not reached an agreement with the peer regarding setting the peer's MRU between the configured minimum and maximum values, the SMS device establishes the PPP session without negotiating the peer's MRU. In that case, the standard MRU of 1500 for PPP circuits, and 1492 for PPP over Ethernet (PPPoE) circuits is used.

Use the **default** form of this command to return the options to their default values.

Examples

The following example sets the peer's minimum and maximum MRU values:

```
[local]RedBack(config)#ppp peer-options mru min 200 max 2000
```

Related Commands

ppp our-options

pppoe client

pppoe client route *ip-address net-mask metric*

no pppoe client route *ip-address net-mask*

Purpose

Configures routes to be installed on the subscriber's PC when multiple Point-to-Point Protocol over Ethernet (PPPoE) sessions exist.

Command Mode

subscriber configuration

Syntax Description

ip-address	IP address of the destination host.
net-mask	Network mask for the route entry.
metric	Cost (number of hops) to this destination.

Default

Routes are not sent to the subscriber's PPPoE client.

Usage Guidelines

Use the **pppoe client** command to configure the Subscriber Management System (SMS) device to provide different routes for different PPPoE sessions. For each PPPoE session, a route is sent in a PPPoE Active Discovery Network (PADN) message, and installed on the subscriber's PC. In this way, subscribers are enabled with seamless client route provisioning on a per-PPPoE session basis. The subsciber's PC client must support PADN. If the PPPoE client ignores the routes, they have no effect.

As an example of this feature, one PPPoE session could provide Internet connectivity, while another session connects corporate headquarters to a remote office site. Routes to the business site might be of a very different nature than the routes that provide access to the Internet.

Use the **no** form of this command to remove the specified route from the configuration.

Examples

The following example specifies that a route at `200.1.1.0 255.255.255.0` is to be used for concurrent multiple PPPoE sessions. This route has a metric, or hop count, of `1`:

```
[local]RedBack(config-sub)#pppoe client route 200.1.1.0 255.255.255.0 1
```

Related Commands

pppoe motm
pppoe url

pppoe motm

pppoe motm *text*

no pppoe motm

Purpose

Enables the sending of a message of the minute (MOTM) to subscribers once their Point-to-Point Protocol over Ethernet (PPPoE) sessions are established and they have been authenticated.

Command Mode

subscriber configuration

Syntax Description

text	Text of the MOTM to be sent to newly authenticated subscribers. The maximum length of an MOTM is 256 characters. Only one MOTM can be active at a time.

Default

None

Usage Guidelines

Use the **pppoe motm** command to send a message to subscribers when their sessions come up. You can use this command to send any information of general use to subscribers. Information about system downtime is one example.

A newly created MOTM overwrites an existing MOTM.

Use the **no** form of this command to delete the MOTM so that the message is no longer sent to subscribers as they initiate sessions.

Examples

The following example establishes an MOTM:

```
[local]RedBack(config-sub)#pppoe motm Network will be down for maintenance from
0100-0400 Saturday.
```

The following example deletes the active MOTM:

```
[local]RedBack(config-sub)#no pppoe motm
```

Related Commands

pppoe url

pppoe services

pppoe services {**all-domains** | **marked-domains**}

{**no** | **default**} **pppoe services**

Purpose

Specifies which domains (services) are advertised to Point-to-Point Protocol over Ethernet (PPPoE) clients.

Command Mode

global configuration

Syntax Description

all-domains	Specifies that all domains are advertised.
marked-domains	Specifies that only domains that have the **advertise** keyword as part of their definition are advertised.

Default

No domains are advertised to PPPoE clients.

Usage Guidelines

Only use the **pppoe services** command if you want to make public the services that the Subscriber Management System (SMS) device provides.

Use the **no** or **default** form of this command to disable domain advertisement.

Examples

The following example enables the advertisement of marked domains to PPPoE clients:

```
[local]RedBack(config)#pppoe services marked-domains
```

Related Commands

domain—context configuration mode

pppoe tag

pppoe tag *tagname string*

default pppoe tag *tagname string*

Purpose

Replaces the default AC-Name PPPoE tag value with the specified string. AC stands for access concentrator.

Command Mode

global configuration

Syntax Description

tagname	PPPoE tag name. Currently, this value must be set to **ac-name**.
string	Alphanumeric string to replace the default value for the AC-Name PPPoE tag.

Default

The Access Operating System (AOS) uses an automatically-generated (and guaranteed to be unique) value for the AC-Name PPPoE tag.

Usage Guidelines

RFC 2516, *Transmitting PPP Over Ethernet*, specifies that the AC-Name PPPoE tag sent in PPPoE Active Discovery Offer (PADO) messages must have a unique value. AOS ensures that this value is unique by creating it from a combination of the backplane serial number and the hostname of the access concentrator device sending the PADO message. When it is desirable to override this default, use the **pppoe tag** command to establish an alternate value for the AC-Name tag. Once you change the default, AOS can no longer guarantee that the value is unique.

Use the **default** form of this command to return the AC-Name value to the automatically-generated default.

Examples

The following example sets the AC-Name tag to `fortune-1`:

```
[local]RedBack(config)#pppoe tag ac-name fortune-1
```

Related Commands

None

pppoe url

pppoe url *url*

no pppoe url

Purpose

Sets the subscriber's Point-to-Point Protocol over Ethernet (PPPoE) client to automatically point the web browser to a specified URL as soon as the session is established.

Command Mode

subscriber configuration

Syntax Description

url	URL to which the subscriber's browser is pointed after the subscriber's PPP session is established. See the "Usage Guidelines" section for special-character sequences that can be used in the *url* argument.

Default

None

Usage Guidelines

Use the **pppoe url** command to point the subscriber's browser to a specific location once the subscriber's PPP session is established.

The value of the *url* argument used in this command is a standard URL that can contain the following special-character sequences. These sequences are expanded by the Subscriber Management System (SMS) device prior to inclusion in a PPP Active Discovery Message (PADM) and can be used to personalize the URL to the subscriber.

- %U—The entire subscriber name used in PPP authentication.
- %u—The user portion of the subscriber name used in PPP authentication. This is the portion of the subscriber name that precedes the first @ or other divider character. If there is no divider character, then %u expands to the entire subscriber name.
- %d—The domain portion of the subscriber name used in PPP authentication. This is the portion of the subscriber name that follows the first @ or other divider character. If there is no divider character, %d expands to a zero length string.
- %D—The name of the context to which the subscriber was authenticated. This may be different than the domain portion of the subscriber name.

- —T%%—Expands to a single% character.

Use the **no** form of this command to remove the URL association from the subscriber record.

Examples

For a subscriber named joe@local, the following example allows a PADM containing the URL `http://www.loe.com/members/joe@local` to be sent to the PPPoE client when the PPP session is established:

```
[local]RedBack(config-ctx)#subscriber name joe
[local]RedBack(config-sub)#pppoe url http://www.loe.com/members/%U
```

For every subscriber to which the subscriber default is applied, the following example sends a PADM containing `http://www.loe.com/members/`*`name`* to the PPPoE client when the PPP session is established:

```
[local]RedBack(config-ctx)#subscriber default
[local]RedBack(config-sub)#pppoe url http://www.loe.com/members/%u
```

Related Commands

pppoe motm

show ip ppp-proxy-arp

show ip ppp-proxy-arp

Purpose

Displays proxy Address Resolution Protocol (ARP) information for Point-to-Point Protocol (PPP) circuits that are bound to a PPP default interface.

Command Mode

operator exec

Syntax Description

This command has no arguments or keywords.

Default

None

Usage Guidelines

Use the **show ip ppp-proxy-arp** command to display proxy ARP information. Ordinarily, PPP sessions that attempt to come up and cannot bind to a valid interface simply fail. A PPP default interface acts as a fallback for those incoming PPP connections. If a PPP session is established, and there is no valid interface to which it can bind, the session binds to the default interface.

Proxy ARP must be enabled on an upstream interface from the PPP default interface. Proxy ARP allows the upstream interface to act as a proxy for PPP sessions that are bound to the PPP default interface. Otherwise, ARP requests destined for PPP sessions are dropped because the IP address of the PPP default interface is always created with a netmask of all ones and, therefore, is never on the same subnet as the PPP sessions that are bound to it.

Examples

The following example displays all PPP proxy ARP table entries:

```
[local]RedBack>show ip ppp-proxy-arp

Host            Nhop cct    Interface

10.1.1.2        18000010    1
20.1.1.2        18010011    2
30.1.1.2        18020012    3
40.1.1.2        18030013    4
```

Related Commands

ip ppp-proxy-arp

show ppp

show ppp [**all**] [{*slot/port* [{[**hdlc-channel** *chan-name*] *dlci* [**through** *end-dlci*] | *vpi* [*vci* [**through** *end-vci*]]} | **subscriber** *sub-name*}] [**summary** | **up** | **down**]

Purpose

Displays a list of Point-to-Point Protocol (PPP) sessions and their current state.

Command Mode

operator exec

Syntax Description

all	Optional. Specifies that information about all contexts is shown. This option is available only to operators and administrators in the local context.
slot/port	Optional. Backplane or midplane slot number and port number of a particular port.
hdlc-channel *chan-name*	Optional. Name of the High-Level Data Link Control (HDLC) channel on a Channelized DS-3 port. This construct is required for Channelized DS-3 modules and not allowed in any other case.
dlci	Optional. Data-link connection identifier (DLCI) number of a configured permanent virtual circuit (PVC).
through *end-dlci*	Optional. Last DLCI number when requesting information for a range of circuits.
vpi	Optional. Virtual path identifier (VPI) of a configured PVC.
vci	Optional. Virtual channel identifier (VCI) of a configured PVC. For ATM T1 modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 modules, the range of values is 1 to 4,095; for all ATM Version 2 modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI number when requesting information for a range of circuits.
subscriber *sub-name*	Optional. Name of the specific subscriber for whom you want PPP information displayed.
summary	Optional. Specifies that only a summary of PVCs is to be displayed. Not available for use with the **subscriber** *name* construct.
up	Optional. Specifies that only PVCs that are active are to be displayed. Not available for use with the **subscriber** *name* construct.

down	Optional. Specifies that only PVCs that are inactive are to be displayed. Not available for use with the **subscriber** *name* construct.

Default

Displays information for the PPP sessions in the current context.

Usage Guidelines

Use the **show ppp** command to display information about PPP sessions. Operators and administrators in the local context can use the **all** keyword to display information on all PPP sessions in all contexts. In all other contexts, only PPP sessions bound to the current context are shown.

If a subscriber name is specified, only PVCs for that subscriber are displayed.

If the optional *slot/port* argument is specified, only the PPP circuits for that port are displayed.

If the value of the *slot/port* argument supports HDLC channels, **hdlc-channel** *chan-name* should be specified to show only the PVCs on a specific channel; otherwise, the PVCs on all HDLC channels on that slot/port are shown.

If the DLCI number is specified (Frame Relay only), only that PVC is shown. If only a single DLCI is specified, the parameters following the DLCI number are not allowed. Use the **through** *end-dlci* construct to specify a range of DLCI numbers to be shown.

If the VPI number is specified (ATM only), only PVCs configured using that VPI are shown. If a VCI is also specified, only that PVC is shown. Use the **through** *end-vci* construct to specify a range of VCIs to be shown.

If the **summary** keyword is specified, only a summary is shown.

If the **up** keyword is specified, only the PVCs that have a Link Control Protocol (LCP) and IP Control Protocol (IPCP) state of opened are shown.

If the **down** keyword is specified, only the PVCs that have an LCP or IPCP state other than opened are shown.

Examples

The following example shows sample output from the **show ppp** command on a Subscriber Management System (SMS) 1000 device. Only sessions in the current context (a) are shown:

```
[a]RedBack>show ppp

Port    PVC     LCP State Auth State IPCP State CCP State Bundle ID Subscriber
----  --------  --------- ---------- ---------- --------- --------- ----------
4/1     2.16    OPENED    NET/PASSED OPENED                        b@a

circuits up:1  circuits down:0  total circuits:1
```

The following example shows sample output from the **show ppp all** command on an SMS 1000 device. Sessions for all contexts are shown:

```
[local]RedBack>show ppp all

Port  PVC       LCP State Auth State IPCP State CCP State Bundle ID Subscriber
----  --------  --------- ---------- ---------- --------- --------- ----------
4/0   2.16      OPENED    NET/PASSED OPENED                        a@b
4/0   2.20      STOPPED   DEAD       INITIAL
4/0   2.21      STOPPED   DEAD       INITIAL
4/0   2.22      STOPPED   DEAD       INITIAL
4/1   2.16      OPENED    NET/PASSED OPENED                        b@a
5/0   0.32      OPENED    NET/PASSED  -ML-       3                 s1@c1
5/0   0.33      OPENED    NET/PASSED OPENED      3                 s1@c1
5/1   0.32      OPENED    NET/PASSED  -ML-       4                 s1@c2
5/1   0.33      OPENED    NET/PASSED OPENED      4                 s1@c2
7/0     77      INITIAL   DEAD       INITIAL
7/0     78      OPENED    NET/PASSED OPENED
7/0     79      INITIAL   DEAD       INITIAL
7/0     80      INITIAL   DEAD       INITIAL

circuits up:7 circuits down:6 total circuits:13
```

The following example shows sample output when a slot, port, VPI, and VCI are specified:

```
[local]RedBack>show ppp 4/0 2 16

Port  PVC       LCP State Auth State IPCP State CCP State Bundle ID Subscriber
----  --------  --------- ---------- ---------- --------- --------- ----------
4/0   2.16      OPENED    NET/PASSED OPENED                        a@b
```

The following example shows sample output from the **show ppp all** command on an SMS 10000 device showing virtual PPPoE sessions:

```
[local]RedBack>show ppp all

Port  PVC       LCP State Auth State IPCP State CCP State Bundle ID Subscriber
----  --------  --------- ---------- ---------- --------- --------- ----------
Virt  00-00001  OPENED    NET/PASSED REQSENT                       a@b
Virt  00-00002  OPENED    NET/PASSED OPENED                        c@b

circuits up:1 circuits down:1 total circuits:2
```

Related Commands

ppp multilink enable
show atm counters
show atm pvc
show bindings
show frame-relay counters
show frame-relay pvc

show ppp compression

show ppp compression [*slot/port* [**counters** | **summary**] | **all** [**counters** | **summary**]] [**subscriber** *name*]

Purpose

Displays Point-to-Point Protocol (PPP) information.

Command Mode

operator exec

Syntax Description

slot/port	Optional. Specific slot and port for which you want information displayed.
counters	Optional. Specifies that you want information about PPP counters included in the display.
summary	Optional. Specifies the display is to include summary information only.
all	Optional. Specifies that you want information for all contexts (as opposed to just the current context) included in the display.
subscriber *name*	Specific subscriber for whom you want information displayed.

Default

None

Usage Guidelines

Use the **show ppp compression** command to display PPP compression information. Use the optional constructs to narrow or broaden the scope of information included in the display.

Examples

The following example shows sample output from the **show ppp compression** command:

```
[local]RedBack>show ppp compression all

SAT FEB 06 22:46:30 2049
             Encode   Encode   Encode   Decode   Decode   Decode
Port PVC     Packets  Ratio    Resets   Packets  Ratio    Resets
---- -------- -------- -------- -------- -------- -------- --------
 6/0 1.32     5        2.7717   0        5        2.8977   0
```

Related Commands

ppp compression

show ppp multilink

show ppp multilink [**all** | **bundle** *bundle-id* | **summary**]

Purpose

Displays multilink Point-to-Point Protocol (MP) state and statistics information.

Command Mode

operator exec

Syntax Description

all	Optional. Displays information for all multilink bundles in all contexts.
bundle *bundle-id*	Optional. Specific multilink bundle for which you want information displayed.
summary	Optional. Displays a summary of all sessions for all contexts.

Default

None

Usage Guidelines

Use the **show ppp multilink** command to display additional information for each session including:

- Link count
- Local maximum received reconstructed unit (MRRU)
- Peer MRRU
- Peer endpoint discriminator

The following statistics are also displayed:

- Fragments dropped
- Fragments outstanding

When used without any optional constructs, this command displays information about all multilink bundles in the current context.

The bundle ID and username associated with each multilink PPP session are displayed in the output of the **show ppp** command.

Examples

The following example shows sample output from the **show ppp multilink** command:

```
[local]RedBack>show ppp multilink

Bundle ID: 4, Link Count: 2 Username: s1@c2
MRRU: 1524, Peer MRRU: 1524
Peer Endpoint-Discriminator: class-3 00:80:50:01:26:77
Fragments Dropped: 0, Fragments Outstanding: 0
```

The following example shows sample output when the **summary** keyword is used:

```
[local]RedBack>show ppp multilink summary

Bundle count = 4, Link count = 2
Total bundles = 10, Total Links = 20
```

Related Commands

ppp multilink enable
show ppp

show pppoe

show pppoe [**all**]

Purpose

Displays information on Point-to-Point Protocol over Ethernet (PPPoE) virtual circuits, including indicating what physical circuit a virtual circuit is on.

Command Mode

operator exec

Syntax Description

all	Optional. Specifies that information is to be displayed for all PPPoE connections regardless of context. This option is available only to operators and administrators in the local context.

Default

Displays information for all PPPoE sessions in the current context.

Usage Guidelines

Use the **show pppoe** command to display information on PPPoE virtual circuits.

This command only shows circuits that are bound to the current context unless the **all** keyword is present. The **all** keyword is only available to administrators and operators in the local context.

Note The virtual circuit number is the same as the PPPoE Session-Id that is contained in each packet.

Examples

The following example shows sample output of the **show pppoe** command on a Subscriber Management System (SMS) 1800 device when the **all** keyword is used:

```
[local]RedBack>show pppoe all

Virtual Circuit     Real Circuit            Subscriber
------------------------------------------------------------
1                   ETHERNET 06.0           dave@ips1
2                   FRAME 04.0.00020        jim@work
4                   ETHERNET 06.0           dan@home
9                   ATM 05.1.010.00010      (no subscriber)
```

The (no subscriber) notation indicates a circuit that either has not yet reached PPP authentication or is on its way down.

The following example shows sample output of the **show pppoe** command on an SMS 10000 device when the **all** keyword is used:

```
[local]RedBack>show pppoe all

Virtual Circuit     Real Circuit            Subscriber
------------------------------------------------------------
00-00001            ETHERNET 00.0           dave@ips1
```

Related Commands

show pppoe counters
show pppoe services

show pppoe counters

show pppoe counters

Purpose

Displays summary statistics for all Point-to-Point Protocol over Ethernet (PPPoE) circuits.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show pppoe counters** command to display a summary of statistics for all PPPoE circuits on the system.

Examples

The following example shows sample output from the **show pppoe counters** command:

```
[local]pm1>show pppoe counters

TUE AUG 10 21:44:58 1999
PPPoE TX/RX packet counters:
                 Transmit                        Receive
                 tx   dropped                    rx   dropped
                 0    0                          0    0

PPPoE PAD counters:
       0 received PADI packets
       0 received PADO packets
       0 received PADR packets
       0 received PADS packets
       0 received PADT packets
       0 received PADM packets
       0 total received PAD packets
       0 total transmited PAD packets
```

```
PPPoE invalid discovery packet counters:
       0 received PAD packets with invalid version/type
       0 received PAD packets with invalid length
       0 received PAD packets with invalid tag length
       0 received PAD packets from server
       0 total received invalid PAD packets
       0 received PAD packets with unknown code
       0 received PADI packets with non-zero session id
       0 received PADR packets with non-zero session id

PPPoE virtual circuit counters:
       0 created virtual circuits
       0 deleted virtual circuits
       0 failed virtual circuits
       0 failed virtual circuit deletes
       0 failed virtual circuit allocations

PPPoE discovery processing counters:
       0 failed PPP init sessions
       0 dropped PADI packets, maximum sessions reached
       0 dropped PADR packets, maximum sessions reached
       0 tags not added because packet too large
       0 received packets on down circuit
       0 received packets with invalid tag service name

PPPoE PADM URL error counters:
       0 malformed URLs
       0 discarded too long expanded URLs
       0 ignoring unsupported expansion character
```

Related Commands

show pppoe
show pppoe services

show pppoe services

show pppoe services

Purpose

Displays the Point-to-Point Protocol over Ethernet (PPPoE) services that are advertised by the system.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show pppoe services** command to display the PPPoE services defined and advertised by the system.

Examples

The following example shows sample output from the **show pppoe services** command:

```
[local]pm1#show pppoe services

        ISP1
        ISP1-gold
        ISP2
        ISP3
```

Related Commands

domain—context configuration mode
pppoe services

Part 6

Tunnels

GRE Commands

This chapter provides the commands used to configure and maintain generic routing encapsulation (GRE) tunnels over IP version 4 (IPv4) and GRE virtual private networks (VPNs) through the Access Operating System (AOS).

For overview information, user tasks, and configuration examples, see the “Configuring GRE” chapter in the *Access Operating System (AOS) Configuration Guide.*

checksum

checksum

no checksum

Purpose

Enables the Access Operating System (AOS) to perform a checksum on generic routing encapsulation (GRE) packets.

Command Mode

GRE peer

Syntax Description

This command has no keywords or arguments.

Default

Checksums are disabled.

Usage Guidelines

Use the **checksum** command to enable the AOS to send checksums in outgoing GRE packets. This mechanism allows the remote system to verify the integrity of each packet. Incoming packets that fail the checksum are discarded.

Modifications to this command do not take effect until you first delete the GRE tunnel using the **clear gre-peer** command.

Use the **no** form of this command to disable checksum.

Examples

The following example enables checksum for GRE packets:

```
[local]RedBack(config-gre)#checksum
```

Related Commands

clear gre peer
gre-peer

clear gre peer

clear gre peer *peer-name* [**key** *key-id* | **all**]

Purpose

Causes the Access Operating System (AOS) to clear existing generic routing encapsulation (GRE) tunnel parameters and apply new parameters.

Command Mode

administrator exec

Syntax Description

peer-name	Name of the GRE peer whose parameters are cleared.
key *key-id*	Optional. Tunnel key to clear and reset. Parameters for the circuit associated with the key are cleared and new parameters are applied.
all	Optional. Clears all tunnel keys and parameters for all tunnel circuits, and applies new parameters globally.

Default

None

Usage Guidelines

Use the **clear gre peer** command to clear existing GRE tunnel parameters and apply new parameters. By specifying the **key** *key-id* construct, you can clear and reset parameters for the specific virtual private network (VPN) that is created when traffic travels between two GRE peers using that particular key. If you do not specify the **key** *key-id* construct, the command applies to the tunnel created with no key.

If you issue the **clear gre peer** command while keys within the GRE tunnel are waiting for authentication, authorization, and accounting (AAA) to learn bind information, the request may time out. When such timeouts occur, existing parameters remain in use.

Examples

The example clears and reapplies VPN parameters for the circuit identified by the key 35:

```
[local]Redback>clear gre peer delphi key 35
```

Related Commands

gre-peer
gre-tunnel

description

description *text*

no description

Purpose

Describes the generic routing encapsulation (GRE) tunnel.

Command Mode

GRE peer

Syntax Description

text	Text string of up to 255 characters in length.

Default

None

Usage Guidelines

Use the **description** command to provide a description of the GRE tunnel.

Use the **no** form of this command to remove a description for a GRE tunnel.

Examples

The following example describes the GRE tunnel as `tocorpA`:

```
[local]RedBack(config-gre)#description tocorpA
```

Related Commands

gre-peer

gre-circuit creation

gre-circuit creation on-demand aaa [*ctx-name*]

Purpose

Places the SMS device in listen mode, enabling the automatic creation of generic routing encapsulation (GRE) tunnels. Also enters GRE creation configuration mode.

Command Mode

tunnel map

Syntax Description

on-demand	Specifies that GRE tunnels are to be created automatically.
aaa	Specifies that AAA is to be used for GRE.
ctx-name	Optional. Name of the context in which to search for GRE tunnel traffic.

Default

None

Usage Guidelines

Use the **gre-circuit creation** command to enable GRE autoconfiguration. Before issuing this command, you must first configure authentication, authorization, and accounting (AAA) to use Remote Authentication Dial-In User Service (RADIUS) for GRE. Use the **aaa authorization gre** command with the **radius** keyword to configure AAA appropriately.

Examples

The following example instructs the SMS device to listen for new GRE tunnels in the context `redback1`:

```
[local]RedBack(config)#tunnel map
[local]RedBack(config-tunnel)#gre-circuit creation on-demand aaa redback1
[local]Redback(config-gre-creation)#
```

Related Commands

aaa authorization gre

gre-peer

gre-peer name *peer-name* **remote** *ip-address* **local** *ip-address*

no gre-peer name *peer-name*

Purpose

Configures a generic routing encapsulation (GRE) tunnel and enters GRE peer configuration mode.

Command Mode

context configuration

Syntax Description

name *peer-name*	Text string of up to 128 characters identifying the GRE tunnel. This name must be unique from all other tunnels, including Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F), and GRE tunnels, that reside in the same context.
remote *ip-address*	IP address of the remote side of the GRE tunnel.
local *ip-address*	IP address of local end of the GRE tunnel.

Default

None

Usage Guidelines

Use the **gre-peer** command to configure a GRE tunnel. You can configure multiple tunnels. The remote IP address at one end of the GRE tunnel is the same as the local IP address on the other end of the GRE tunnel and vice versa. The **local** *ip-address* construct must match the IP address of an interface in the same context in which the **gre-peer** command is entered. Use the **gre-tunnel** command to configure the GRE tunnel circuit.

Use the **no** form of this command to remove the specified GRE tunnel and any associated parameters that have been configured in GRE peer configuration mode.

Examples

The following example configures a GRE tunnel called `toCorpB` with a remote IP address of `10.0.0.2`, and a local IP address of `10.0.0.1`:

```
[local]RedBack(config-ctx)#gre-peer name toCorpB remote 10.0.0.2 local 10.0.0.1
[local]RedBack(config-gre)#
```

Related Commands

clear gre peer
gre-tunnel
show gre tunnel counters
show gre tunnel info

gre-rpf-check

gre-rpf-check

Purpose

Enables reverse path forwarding (RPF) check to ensure that the incoming generic routing encapsulation (GRE) packet is received on an interface which is a candidate outbound interface for the return route.

Command Mode

GRE creation configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **gre-rpf-check** command to ensure that an incoming GRE packet is received on an interface which is a candidate outbound interface for the return route. For example if a GRE packet with a source IP address of 1.1.1.1 is received on interface eth0, the system ensures that a return path to IP address 1.1.1.1 exists through interface eth0.

Examples

The following example enables RPF check:

```
[local]Redback(config-gre-creation)#gre-rpf-check
```

Related Commands

gre-circuit creation

gre-tunnel

gre-tunnel *tun-name ctx-name* [**key** *key-id*] [**server**]

no gre-tunnel *tun-name ctx-name*

Purpose

Identifies the generic routing encapsulation (GRE) tunnel that will be mapped to a circuit and enters tunnel circuit configuration mode.

Command Mode

tunnel map

Syntax Description

tun-name	Name of a configured GRE peer that has been created through the **gre-peer** command, or defined via Remote Authentication Dial-In User Service (RADIUS) attributes.
ctx-name	Name of the context in which the GRE peer is defined.
key *key-id*	Optional. Value, in integer form, that specifies a virtual private network (VPN) key. The range of values is 1 to 4,294,967,295; the default value is to have no key associated with the tunnel.
server	Optional. Causes the tunnel circuit to behave as the server side of a tunnel.

Default

None

Usage Guidelines

Use the **gre-tunnel** command to identify the GRE tunnel that will be mapped to a circuit via the **bind interface** command in tunnel circuit configuration mode. The GRE tunnel is treated like a virtual circuit that is bound to an interface in a context.

Use the **key** *key-id* construct to specify the VPN that is created when traffic travels between two GRE peers using that particular key. When you use this construct, the GRE header includes the key option. If no key is specified, no key option is included.

If the **server** keyword is specified for a particular tunnel, all keys for that tunnel must also be configured with the **server** keyword, or tunnel creation fails. If at any point a Remote Dial-In User Server (RADIUS) query fails, or if consistency checks fail for the attributes, configuration of the tunnel key circuit fails and a message is recorded in the system log.

You can bind multiple GRE tunnels to the same interface, in which case, you can use the **ip host** command in tunnel circuit configuration mode to indicate the IP address of the remote interface.

Use the **no** form of this command to remove the GRE tunnel mapping.

Examples

The following example binds two GRE tunnels to the `upstream` interface in the `vpn1` context. The example uses the **ip host** commands to specify the addresses reachable through each tunnel:

```
[local]RedBack(config)#tunnel map
[local]RedBack(config-tunnel)#gre-tunnel toBoston local key 1234
[local]RedBack(config-tun-circuit)#bind interface upstream vpn1
[local]RedBack(config-tun-circuit)#ip host 1.1.1.2
.
.
.
[local]RedBack(config-tunnel)#gre-tunnel toDallas local key 5678
[local]RedBack(config-tun-circuit)#bind interface upstream vpn1
[local]RedBack(config-tun-circuit)#ip host 1.1.1.3
```

Related Commands

aaa authorization gre
clear gre peer
gre-peer
ip host—tunnel circuit configuration mode

ip host

ip host *ip-address*

no ip host *ip-address*

Purpose

Creates a static host entry in the system host table.

Command Mode

tunnel circuit configuration

Syntax Description

ip-address	IP address of the host.

Default

None

Usage Guidelines

Use the **ip host** command to install permanent entries in the host table. This is useful in the case where multiple generic routing encapsulation (GRE) tunnels are bound to a single interface. This command indicates the IP address of the remote interface to which a tunnel is bound.

A GRE tunnel, which acts like a virtual circuit, must be bound to an interface with the **bind interface** command in tunnel circuit configuration mode.

Use the **no** form of this command to remove the specified entry from the host table.

Note This command is also described in Chapter 9, “Common Port, Circuit, and Channel Commands” and Chapter 10, “Ethernet Port Commands.”

Examples

The following example configures a host entry for the IP address `10.1.1.254`:

```
[local]RedBack(config)#tunnel map
[local]RedBack(config-tunnel)#gre-tunnel toBoston local key 1234
[local]RedBack(config-tun-circuit)#bind int eth1 toBoston
[local]RedBack(config-tun-circuit)#ip host 10.1.1.254
```

Related Commands

show ip host

police

police rate *rate* **burst** *size*

no police

Purpose

Limits, by rate and burst tolerance, the aggregate packet stream received on a generic routing encapsulation (GRE) tunnel.

Command Mode

GRE peer configuration

Syntax Description

rate *rate*	Limit rate in kbps. The range of values is 10 to 155,520.
burst *size*	Burst tolerance size in bytes. The range of values is 0 to 100,000.

Default

None

Usage Guidelines

Use the **police** command to limit the aggregate packet stream received over a GRE tunnel. A general rule to determine burst tolerance is to multiply the link maximum transmission unit (MTU) by 10 (approximately 15,000 to 20,000 bytes for subscriber circuits). A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and burst tolerance are dropped.

Modifications to this command do not take effect until you first delete the GRE tunnel using the **clear gre-peer** command.

Use the **no** form of this command to remove the traffic limitations.

Examples

The following example sets limitations on the rate and burst size of incoming traffic through the tunnel:

```
[local]RedBack(config-ctx)#gre-peer name toBoston
[local]RedBack(config-gre)#police rate 12 burst 17000
```

Related Commands

gre-peer
rate-limit—GRE peer configuration mode

rate-limit

rate-limit rate *rate* **burst** *size*

no rate-limit

Purpose

Limits, by rate and burst tolerance, the aggregate packet stream sent out a generic routing encapsulation (GRE) tunnel.

Command Mode

GRE peer configuration

Syntax Description

rate *rate*	Limit rate in kbps. The range of values is 10 to 155,520 kbps.
burst *size*	Burst tolerance size in bytes. The range of values is 0 to 100,000 bytes.

Default

There is no limitation on the rate and burst size of outgoing traffic.

Usage Guidelines

Use the **rate-limit** command to limit the aggregate packet stream sent out a GRE tunnel. A general rule to determine burst tolerance is to multiply the link maximum transmission unit (MTU) by 10 (approximately 15,000 to 20,000 bytes for subscriber circuits). A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and burst tolerance are dropped.

Modifications to this command do not take effect until you first delete the GRE tunnel using the **clear gre-peer** command.

Use the **no** form of this command to remove the traffic limitations.

Examples

The following commands set limitations on the rate limit and burst size of traffic sent out the tunnel:

```
[local]RedBack(config-ctx)#gre-peer name toBoston
[local]RedBack(config-gre)#rate-limit rate 12 burst 17000
```

Related Commands

gre-peer
police—GRE peer configuration mode

show gre counters

show gre counters peer *peer-name* [**key** *key-id* | **all**]

Purpose

Displays statistics for generic routing encapsulation (GRE) tunnel keys.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Name of the peer about which you want to display information.
key *key-id*	Optional. Key associated with the virtual private network (VPN) for which counters information is to be displayed. The range of values is 1 to 4,294,967,295; the default is to have no key.
all	Displays information for all keys on the tunnel.

Default

Information for all GRE tunnels is displayed.

Usage Guidelines

Use the **show gre counters** command with no keywords to display statistics for all GRE tunnels. Use the **peer** *peer-name* construct to display detailed information for the specified GRE peer. Use the **key** *key-id* construct to display detailed information for the VPN that uses the specified key. If you do not specify the **key** *key-id* construct, the command applies to the tunnel created with no key. Use the **all** keyword to display information for all keys on the tunnel.

Table 24-1 describes **show gre counters** command output fields.

Table 24-1 show gre counters Command Field Descriptions

Field	Description
Tx Data Packets	Number of data packets transmitted by the peer
Rx Data Packets	Number of data packets received by the peer
Tx Data Bytes	Number of data bytes transmitted by the peer
Rx Data Bytes	Number of data bytes received by the peer
Police pkt drops	Number of packets dropped by the peer due to police limit
Rate pkt drops	Number of packets dropped by the peer due to rate limit

Examples

The following example displays sample output for the **show gre counters** command for the peer `toBoston` for the circuit identified by the key `5010`:

```
[local]RedBack>show gre counters peer toBoston key 5010

Tx Data Packets:             20         Rx Data Packets:           105
Tx Data Bytes:               2480       Rx Data Bytes:             13020
```

The following example displays sample output for the **show gre counters** command for the peer `toBoston`, using the **all** keyword:

```
[local]RedBack>show gre counters peer toBoston all

Tx Data Packets:             500        Rx Data Packets:           221
Tx Data Bytes:               62000      Rx Data Bytes:             27404
Police pkts drops:           15         Rate pkts drops:           0
```

Related Commands

clear gre peer
gre-peer
show gre tunnel counters

show gre info

show gre info peer *peer-name* [**key** *key-id* | **all**]

Purpose

Displays generic routing encapsulation (GRE) tunnel keys information.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Name of the GRE peer for which information is displayed.
key *key-id*	Optional. Key that is associated with the virtual private network (VPN) for which information is displayed.
all	Displays information for all keys on the tunnel.

Default

Displays information for all GRE tunnels in the current context.

Usage Guidelines

Use the **show gre info** command to display GRE tunnel information. Use the **peer** *peer-name* construct to display detailed information for the specified GRE peer. Use the **key** *key-id* construct to display detailed information for the VPN that uses the specified key. If the **key** *key-id* construct is not specified, the command applies to the tunnel created with no key. Use the **all** keyword to display information for all keys on the tunnel.

Examples

The following example provides sample output for the **show gre info** command for the peer named `toBoston` for the circuit identified by the key `5010`:

```
[local]RedBack>show gre info peer toBoston key 5010

key 5010 is bound to interface vpn1 in context corp1
```

The following example provides sample output for the **show gre info** command for the peer named `toBoston`, using the **all** keyword:

```
[local]RedBack>show gre info peer toBoston all

Tunnel Key     State        Interface Name        Context
-----------    ---------    ------------------    -----------
5020           Bound        vpn2                  corp2
5010           Bound        vpn1                  corp1
```

Related Commands

clear gre peer
gre-peer
show gre tunnel info

show gre tunnel counters

show gre tunnel counters [**peer** *peer-name*]

Purpose

Displays statistics for generic routing encapsulation (GRE) tunnels.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Optional. Name of the peer about which you want information displayed.

Default

Information for all GRE tunnels is displayed.

Usage Guidelines

Use the **show gre tunnel counters** command with no keywords to display statistics for all GRE tunnels. Use the **peer** *peer-name* construct to display information for a specific GRE peer only.

Examples

The following example displays the output for the **show gre tunnel counters** command for all peers in the local context:

```
[local]RedBack>show gre tunnel counters

Peer Name            Tx Pkts         Rx Pkts
-------------------- --------------- ---------------
peertest1            2009948         83729993
peertest2            230985          0
```

Related Commands

clear gre peer
gre-peer
show gre counters

show gre tunnel info

show gre tunnel info [**peer** *peer-name*]

Purpose

Displays generic routing encapsulation (GRE) tunnel information.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Optional. Name of the GRE peer for which you want information displayed.

Default

Displays information for all GRE tunnels in the current context.

Usage Guidelines

Use the **show gre tunnel info** command to display GRE tunnel information. Use the **peer** *peer-name* construct to display information for a specific GRE peer only.

Table 24-2 describes the **show gre info** command output fields when you specify a particular tunnel peer.

Table 24-2 show gre info Command Field Descriptions

Field	Description
Remote IP address	Remote IP address of the peer as entered in the **gre-peer** command
Local IP address	Local IP address of the peer as entered in the **gre-peer** command
Checksum	GRE checksum
Bind state	GRE circuit state
Police rate	User-set value for police rate
Police burst	User-set value for police burst
Rate-limit-rate	User-set value for limit rate
Rate-limit-burst	User-set value for limit burst

Examples

The following example displays information for all tunnels in the context:

```
[local]RedBack>show gre tunnel info

Peer Name            remote addr     local addr       state
-------------------- --------------- ---------------  --------
toBoston             2.2.2.2         1.1.1.1          Configured
toSJ                 4.4.4.4         3.3.3.3          Configured
```

The following example displays information for a specific tunnel:

```
[local]RedBack>show gre tunnel info peer toBoston

Remote IP address: 2.2.2.2         Local IP address: 1.1.1.1
Checksum:          Disabled        Tunnel state:     Configured
Police rate:       0               Police burst:     0
Rate-limit-rate:   0               Rate-limit burst: 0
```

Related Commands

clear gre peer
gre-peer
show gre info

tunnel map

tunnel map

Purpose

Enters generic routing encapsulation (GRE) tunnel map configuration mode.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **tunnel map** command to enter GRE tunnel map configuration mode.

Examples

The following example changes the command mode from interface configuration mode to GRE tunnel map configuration mode:

```
[local]RedBack(config)#tunnel map
[local]RedBack(config-tunnel)#
```

Related Commands

gre-circuit creation
gre-tunnel

L2TP Commands

This chapter describes the commands related to configuring Layer 2 Tunneling Protocol (L2TP) peers and groups. L2TP peers (including unnamed and default peers) are configured in the L2TP configuration mode. Use the **l2tp-peer name**, **l2tp-peer unnamed**, or **l2tp-peer default** context configuration mode command to access the L2TP configuration mode. Groups of L2TP Network Server (LNS) peer members are configured in the L2TP group configuration mode. Use the **l2tp-group name** context configuration mode command to access the L2TP group configuration mode.

Note Unless otherwise indicated in the documentation for individual commands, changing the configuration of a peer with an established tunnel takes effect only upon issuing a **clear tunnel** command.

For overview information, a description of the tasks used to configure L2TP peers, and configuration examples, see the "Configuring L2TP" chapter in the *Access Operating System (AOS) Configuration Guide*.

algorithm

algorithm {**first** | **load-balance**}

default algorithm

Purpose

Specifies the algorithm used to distribute Point-to-Point Protocol (PPP) sessions among the peers in a Layer 2 Tunneling Protocol (L2TP) group.

Command Mode

L2TP group configuration

Syntax Description

first	Specifies the algorithm as strict-priority where one peer is used until or unless connectivity to that peer is lost. The next peer in line is then used.
load-balance	Specifies the algorithm as load-balancing where sessions are distributed across the peers equally.

Default

The algorithm is set to strict-priority.

Usage Guidelines

Use the **algorithm** command to specify the algorithm you want used to distribute PPP sessions among peers in an L2TP group. The two algorithm options represent distinctly different strategies for session distribution.

For strict-priority, each peer is assigned a priority. At the command-line interface (CLI), the priorities correspond to the order in which the peers are listed—the highest priority peer being listed first. Sessions are directed to the highest priority peer until connection with that peer is no longer possible, and then sessions are directed to the peer with the next highest priority.

The distribution of sessions works differently when the load-balancing algorithm is selected. In that case, the peer with the fewest sessions gets the next session. The result is that the sessions are distributed across the peers more or less equally. The peers may still have priorities assigned, but they are ignored.

Both algorithms are subject to the maximum number of tunnels (**max-tunnels** command), and maximum number of sessions (**max-sessions** command) configured for the peers that are members of the group. For example, if strict-priority is being used and the maximum sessions limit is reached on the highest priority peer, additional sessions are sent to the next highest priority peer.

There are some significant considerations for Remote Authentication Dial-In User Service (RADIUS)-based configurations of L2TP groups resulting from the requirement that both types of RADIUS servers be supported—those that support tunnel extensions (tunnel tags) and those that do not.

Servers That Do Not Support Tunnel Extensions

The following is an example of a RADIUS tunnel configuration for a server that does not support tunnel extensions. The L2TP group is named `isp` and the peer members are `peer1`, `peer2`, and `peer3`. The Tunnel-Preference attribute determines which tunnel has the highest priority for the case of strict priority. Lower preference numbers mean higher priority. If the Tunnel-Preference attribute is missing from all peers, the server-dependent order in which the peers are listed becomes the priority order. We highly recommend setting the priority explicitly. In the case that some peers have an explicit priority and some do not, the ones without priorities are considered of lower priority than those with explicit priorities. In the example below, `peer2` is the highest-priority peer, because it has the lowest preference value. The examples shown here represent a vendor-specific implementation (Merit server).

```
isp
Password = “Redback”,
Service-type = Outbound,
RedBack:Tunnel-Algorithm = 1
RedBack:Tunnel-Deadtime = 10,
RedBack:Tunnel-Group = TRUE,
RedBack:Tunnel-Name = “peer2”,
RedBack:Tunnel-Name = “peer3”,
RedBack:Tunnel-Name = “peer1”

peer1
Password = “Redback”,
Service-type = Outbound,
Tunnel-Medium-Type = IP,
Tunnel-Client-Endpoint =12.1.1.1,
Tunnel-Server-Endpoint = 12.1.1.5,
Tunnel-Password = “pass4me”,
Tunnel-Preference = 3,
Redback:Tunnel_Local_Name = “gr-atm1”

peer2
Password = “Redback”,
Service-type = Outbound,
Tunnel-Medium-Type = IP,
Tunnel-Client-Endpoint =22.1.1.1,
Tunnel-Server-Endpoint = 22.1.1.5,
Tunnel-Password = “pass4me”,
Tunnel-Preference = 1,
Redback:Tunnel_Local_Name = “gr-atm2”

peer3
Password = “Redback”,
Service-type = Outbound,
Tunnel-Medium-Type = IP,
Tunnel-Client-Endpoint =32.1.1.1,
Tunnel-Server-Endpoint = 32.1.1.5,
```

```
Tunnel-Password = “pass4me”,
Tunnel-Preference = 2,
Redback:Tunnel_Local_Name = “gr-atm3”
```

Servers That Do Support Tunnel Extensions

The following is an example of a RADIUS tunnel configuration for a server that does support tunnel extensions (tunnel tags). The Tunnel-Preference attribute determines which tunnel has the highest priority for the case of strict-priority. Lower preference numbers mean higher priority. In the example below, the tunnel with tag 1 is the highest-priority peer, because it has the lowest preference value. If the Tunnel-Preference attribute is missing from all peers, the tag value becomes the priority order (i.e., the lowest-tag-numbered peer becomes the highest-priority peer). We highly recommend setting the priority explicitly rather than overloading the tag field. In the case that some peers have a priority and some do not, the ones without priorities are considered of lower priority than those with explicit priorities.

```
isp
Password = “Redback”,
RedBack:Tunnel-Deadtime = 10,
Service-type = Outbound,
Tunnel-Medium-Type = 1:IP,
Tunnel-Client-Endpoint = 1:12.1.1.1,
Tunnel-Server-Endpoint = 1:12.1.1.5,
Tunnel-Password = 1:“pass4me”,
Tunnel-Preference = 1:3,
Redback:Tunnel_Local_Name = 1:“gr-atm”
Tunnel-Medium-Type = 2:IP,
Tunnel-Client-Endpoint = 2:22.1.1.1,
Tunnel-Server-Endpoint = 2:22.1.1.5,
Tunnel-Password = 2:“pass4me”,
Tunnel-Preference = 2:3,
Redback:Tunnel_Local_Name = 2:“gr-atm”
Tunnel-Medium-Type = 3:IP,
Tunnel-Client-Endpoint = 3:32.1.1.1,
Tunnel-Server-Endpoint = 3:32.1.1.5,
Tunnel-Password = 3:“pass4me”,
Tunnel-Preference = 3:3,
Redback:Tunnel_Local_Name = 3:“gr-atm”
```

The names of the individual peers can be anonymous for User Datagram Protocol (UDP)/IP tunnels. The names of the tunnels are assigned as groupname_tag. For example, the name for the first tunnel in the previous example would be assigned as isp_1.

However, in the case of permanent virtual circuit (PVC)-based tunnels (Tunnel-Medium-Type = PVC), the above mechanism would not suffice, because the **bind l2tp-tunnel** command requires an explicit peer name. In such a case, the Tunnel-Assignment-Id RADIUS attribute is used to associate a specific peer with the one named in the **bind l2tp-tunnel** command.

Changing the configuration of a peer group with established tunnels does not take effect until you delete all tunnels to the peers (using the **clear tunnel** command), or until all the tunnels to all the peers in the group come down naturally. The configuration database is queried again to reestablish tunnels to the peers, thereby implementing the new configuration.

Use the **default** form of this command to set the algorithm to strict-priority.

Examples

The following example creates an L2TP group named `group1` with L2TP peer members `1peer` and `2peer`. Sessions with usernames of the form *user*@group1 would be tunneled to `1peer` (because it is listed first in the group definition) as long as `1peer` is reachable and its max-sessions parameter has not been exceeded. If `1peer` should become unreachable or its max-sessions parameter is reached, sessions would be tunneled to `2peer`.

First, the L2TP group `group1` is created. Two peer members, `1peer` and `2peer`, are then established as members of the group, and the group is configured to use strict-priority session parceling:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tpgrp)#peer-name 1peer
[local]RedBack(config-l2tpgrp)#peer-name 2peer
[local]RedBack(config-l2tpgrp)#algorithm first
```

Related Commands

bind l2tp-tunnel
clear tunnel
deadtime
description
domain
l2tp attribute calling-number real-circuit-id
max-sessions
max-tunnels
peer-name
show l2tp info
show l2tp group

clear tunnel

clear tunnel {**group** *group-name* | **peer** *peer-name* [**tunnel** *tunnel-id* [**session** *session-id*]]}

Purpose

Shuts down all or specified tunnels or sessions to a Layer 2 Tunneling Protocol (L2TP) peer, Layer 2 Forwarding (L2F) peer, or to the members of an L2TP group.

Command Mode

administrator exec

Syntax Description

group *group-name*	Name of an L2TP group.
peer *peer-name*	Name of an L2TP or L2F peer.
tunnel *tunnel-id*	Optional when you use the **peer** *peer-name* construct. Tunnel number of a particular L2TP or L2F tunnel to be shut down.
session *session-id*	Optional when you use the **peer** *peer-name* construct. Session number of a particular L2TP or L2F session to be shut down.

Default

No tunnels are cleared.

Usage Guidelines

Use the **clear tunnel** command to clear L2TP or L2F tunnels or sessions. You can shut down all tunnels to a specified peer if you use the **clear tunnel** command without any optional parameters. To shut down a specific tunnel and all the sessions within that tunnel, specify it by using the **tunnel** *tunnel-id* construct. To shut down a specific session, specify the tunnel and session by using both optional constructs.

For L2TP groups, this command allows you to clear all sessions and tunnels connected to the members of the group. Although all sessions and tunnels are cleared from members of the group, the group itself remains intact.

For Remote Authentication Dial-In User Service (RADIUS)-based configuration, this command is useful when you want to start using a new configuration. After this command is executed, the next RADIUS connection reads the new configuration.

Examples

The following command clears all tunnels to an L2TP peer named `lns.net`:

```
[local]RedBack#clear tunnel peer lns.net
```

The following command clears all tunnels and sessions to all members of the L2TP group called `group1`:

```
[local]RedBack#clear l2tp group group1
```

Related Commands

show l2tp counters
show l2tp group
show l2tp info

deadtime

deadtime *minutes*

default deadtime

Purpose

Sets the minimum amount of time for which the individual peers within a Layer 2 Tunneling Protocol (L2TP) group are marked as “dead” after it is determined that a new tunnel cannot be established to the peer.

Command Mode

L2TP group configuration

Syntax Description

minutes	Minimum number of minutes that a peer is marked as “dead.” The default value is 5.

Default

The deadtime is set to five minutes.

Usage Guidelines

Use the **deadtime** command to set the minimum amount of time that a peer is marked as dead once it is determined that a new tunnel cannot be established to the peer. A peer to which a new tunnel cannot be established is labeled as “dead” in the output of the **show l2tp group** command for at least the length of time indicated in the *minutes* argument. This prevents a troubled L2TP peer from being inundated with connection attempts without disconnecting the peer altogether. It also allows you to identify peers that may be having trouble. Once the deadtime is expired, the next request to connect to the peer is attempted. If not successful, deadtime is again applied to the peer.

Note Current sessions to the peer are not brought down if the peer should be marked as “dead.” Only attempts to add new tunnels are affected.

Use the **default** form of this command to set the deadtime to five minutes.

Changing the configuration of a peer group with established tunnels does not take effect until you delete all tunnels to the peers (using the **clear tunnel** command), or until all the tunnels to all the peers in the group come down naturally. The configuration database is queried again to reestablish tunnels to the peers, thereby implementing the new configuration.

Examples

The following example selects (or creates) an L2TP group and sets the number of deadtime minutes to five:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tpgrp)#default deadtime
```

The following example selects (or creates) an L2TP group and sets the number of deadtime minutes to `10`:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tpgrp)#deadtime 10
```

Related Commands

algorithm
clear tunnel
description
domain
l2tp attribute calling-number real-circuit-id
peer-name
show l2tp group
show l2tp info

debug l2x

debug l2x {**aaa** | **all** | **filter** | **packets** | **ses-setup** | **ses-state** | **tun-setup** | **tun-state** | **window**}

no debug l2x {**aaa** | **all** | **filter** | **packets** | **ses-setup** | **ses-state** | **tun-setup** | **tun-state** | **window**}

Purpose

Enables the logging of Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F) debugging messages.

Command Mode

administrator exec

Syntax Description

aaa	Enables L2TP and L2F authentication, authorization, and accounting (AAA) debugging.
all	Enables all L2TP and L2F debugging.
filter	Configures an L2TP and L2F debugging filter.
packets	Enables L2TP and L2F packet-level debugging.
ses-setup	Enables L2TP and L2F session-setup debugging.
ses-state	Enables L2TP and L2F session state-change debugging.
tun-setup	Enables L2TP and L2F tunnel-setup debugging.
tun-state	Enables L2TP and L2F tunnel state-change debugging.
window	Enables L2TP and L2F control-window debugging.

Default

L2TP and L2F debugging are disabled.

Usage Guidelines

Use the **debug l2x** command to enable the logging of L2TP and L2F debug messages. Use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable L2TP and L2F debugging.

Examples

The following command enables all types of debug logging for L2TP and L2F:

```
[local]RedBack#debug l2x all
```

Related Commands

l2tp attribute calling-number real-circuit-id
l2tp-peer name
l2tp-peer unnamed
logging console
show debugging
terminal monitor
tunnel domain
tunnel name

description

description *text*

no description

Purpose

Creates a textual description of a Layer 2 Tunneling Protocol (L2TP) peer or group.

Command Mode

L2TP configuration
L2TP group configuration

Syntax Description

text	Textual description of an L2TP peer. May be any alphanumeric string, including spaces, that is not longer than one line. The text does not wrap to the next line.

Default

No description is associated with the peer or group.

Usage Guidelines

Use the **description** command to associate descriptive information with the name of the L2TP peer or group. The description appears in the output of the **show configuration** command.

Use the **no** form of this command to delete an existing description. Because there can be only one description per peer or group, when you use the **no** form of this command, it is not necessary to include the *text* argument.

To change a description, create a new one, and it overwrites the existing one.

Examples

The following example specifies (or creates) an L2TP group and then attaches a text description to it:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tp)#description Washington only
```

The following example specifies (or creates) an L2TP peer and then attaches a text description to it:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#description LNS in Washington
```

The following example changes the description created in the previous example:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tpgrp)#description LNS in Washington state
```

The following example removes an existing description:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#no description
```

Related Commands

l2tp attribute calling-number real-circuit-id
l2tp-peer name
show configuration

dnis

dnis [**only**]

{**no** | **default**} **dnis**

Purpose

Enables tunnel switching based on the Dialed Number Identification Service (DNIS) attribute of Layer 2 Tunneling Protocol (L2TP) sessions.

Command Mode

L2TP configuration

Syntax Description

only	Optional. Specifies that the DNIS attribute must be present on incoming sessions for the sessions to be accepted.

Default

Tunnel switching based on the DNIS attribute is disabled.

Usage Guidelines

Use the **dnis** command for tunnel switching applications only. DNIS is primarily used for tunnel switching dialup users (for example, aggregation of traffic from multiple dial-up remote access server (RAS) units into one or multiple tunnels).

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** or **default** form of this command to disable DNIS attribute-based tunnel switching.

Examples

The following example selects (or creates) an L2TP peer and then enables DNIS attribute-based tunnel switching on that peer:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#dnis
```

Related Commands

clear tunnel
show l2tp counters
show l2tp info

domain

domain *dom-name*

no domain *dom-name*

Purpose

Creates an alias for a Layer 2 Tunneling Protocol (L2TP) peer or group. You can use the alias anywhere that you can use the *peer-name* argument from the **l2tp-peer name** command or the *group-name* argument from the **l2tp-group name** command.

Command Mode

L2TP configuration
L2TP group configuration

Syntax Description

dom-name	Name to be used as an alias. Cannot be a name that is already being used as an L2TP peer name, an L2TP group name, a peer domain name, or a group domain name.

Default

No aliases are created.

Usage Guidelines

Use the **domain** command to create simpler names (for example, isp.net) than the *peer-name* argument, which is a fully qualified domain name (for example, hssi_0_5.chi_core.isp.net). You may configure multiple domains per L2TP peer or group.

When using Dialed Number Identification Service (DNIS)-based tunnel selection (see the **dnis** command), you must use the **domain** command to create aliases for outgoing tunnels that match the DNIS (for example, the phone number). For example, to use a tunnel named corp.com for all sessions that provide a DNIS of (888) 555-1212, include the **domain 8885551212** command within the tunnel configuration of the corp.com peer. The **domain** alias and DNIS must exactly match. You must use the **domain** command at the context level if the outgoing tunnel is in a context other than the incoming tunnel.

You cannot use this command if you entered L2TP configuration mode using either the **l2tp-peer unnamed** command or the **l2tp-peer default** command.

An L2TP peer domain name may not be the same as an existing L2TP peer name, L2TP group name, L2TP peer domain name, or L2TP group domain name. Maintain unique names for all groups, peers, and domains.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to remove the specified domain name as an alias.

Examples

The following example selects (or creates) an L2TP peer and creates a domain name (alias) for it:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#domain corporate
```

The following example selects (or creates) an L2TP group and creates a domain name for it:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tp)#domain tier one support
```

Related Commands

clear tunnel
dnis
l2tp attribute calling-number real-circuit-id
l2tp-peer name
show l2tp counters
show l2tp info

ethernet encapsulation

ethernet encapsulation ppp over-ethernet

default ethernet encapsulation

Purpose

Specifies the type of Ethernet encapsulation to be used for any Ethernet traffic on the Layer 2 Tunneling Protocol (L2TP) peer.

Command Mode

L2TP configuration

Syntax Description

ppp over-ethernet	Specifies that the type of Ethernet encapsulation to be used is Point-to-Point Protocol over Ethernet (PPPoE).

Default

If this command is not used, peer encapsulation is set to IP bridging for Ethernet over L2TP sessions.

Usage Guidelines

Use the **ethernet encapsulation** command to enable Ethernet encapsulated sessions through L2TP tunnels.

At this time, PPPoE is the only encapsulation option available using this command. If this command is not issued, the encapsulation for the peer is set to IP bridging for Ethernet over L2TP sessions.

Use the **default** form of this command to reset the encapsulation to IP bridging.

Examples

The following example sets the Ethernet encapsulation on an L2TP peer to PPPoE:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#ethernet encapsulation ppp over-ethernet
```

Related Commands

l2tp-peer name
l2tp-peer unnamed
show l2tp info

ethernet session

ethernet session {{**auth** {**pap** | **chap** | **chap pap**} [**maximum** *sessions*] [**context** *ctx-name* | **service-group** *group-name*]} | **interface** *if-name ctx-name*}

no ethernet session

Purpose

Specifies the authentication method to be used for the Ethernet session on the Layer 2 Tunneling Protocol (L2TP) peer.

Command Mode

L2TP configuration

Syntax Description

auth	Specifies that an authorization protocol is being selected. Must be followed by either the **pap**, **chap**, or **chap pap** keywords. The **auth** construct is only available when the session is PPPoE with Ethernet encapsulation.
pap	Specifies that Password Authentication Protocol (PAP) is to be used to obtain the username and password from the subscriber.
chap	Specifies that Challenge Handshake Authentication Protocol (CHAP) is to be used to obtain the username and password from the subscriber.
chap pap	Specifies that either PAP or CHAP can be used to obtain the username and password from the subscriber, but that CHAP is preferred.
maximum *sessions*	Optional. Maximum number of Point-to-Point Protocol over Ethernet (PPPoE) sessions allowed per L2TP session. The range of values is 0 (which means there is no maximum) to 8,000; the default value is 0.
context *ctx-name*	Optional. Restricts PPPoE sessions with Ethernet encapsulation on the circuits and ports being bound to the specified context.
service-group *group-name*	Optional. Limits the services available to the circuit or port to those permitted by the named service access list.
interface *if-name ctx-name*	Name of the interface to which the Ethernet session is to be bound and the name of the context within which the interface exists. Only available if the session is something other than PPPoE with Ethernet encapsulation.

Default

No Ethernet session authentication method is set.

Usage Guidelines

Use the **ethernet session** command to specify the authentication method to be used for the Ethernet session on the L2TP peer. The **auth** and **interface** constructs are mutually exclusive. The **auth** construct is only available when the session is PPPoE with Ethernet encapsulation; otherwise, the **interface** construct is available. The authentication controlled by the **auth** construct is only for the Ethernet-encapsulated PPPoE session carried by the tunnel, not any PPP sessions that might also be present. For the PPP sessions, the **session-auth** command controls the authentication method.

Use the **no** form of this command to remove the setting from the configuration.

Examples

The following example shows setting the authentication method for an Ethernet-encapsulated PPPoE session:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#ethernet session auth chap pap
```

Related Commands

l2tp-peer name
l2tp-peer unnamed
session-auth
show l2tp info

function

function {**lac-only** | **lns-only**}

no function

Purpose

Specifies that only Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) or L2TP network server (LNS) be enabled for an L2TP peer.

Command Mode

L2TP configuration

Syntax Description

lac-only	Specifies that only LAC is enabled for an L2TP peer.
lns-only	Specifies that only LNS is enabled for an L2TP peer.

Default

LAC and LNS are both enabled for an L2TP peer.

Usage Guidelines

Use the **function** command to specify either LNS or LAC functionality on a peer. Disabling LNS functionality prevents the acceptance of Incoming-Call-Request (ICRQ) control messages from a LAC peer. Disabling LAC functionality prevents the generation of ICRQ control messages based on incoming PPP sessions to the peer.

Note We recommend that you specify the **lns-only** keyword if you are configuring support for anonymous tunnels.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to disable any specification so the peer functions as both LNS and LAC.

Examples

The following example configures the named L2TP peer to function only as a LAC:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#function lac-only
```

Related Commands

clear tunnel
l2tp-peer name
l2tp-peer unnamed
show l2tp info

ipsec peer

ipsec peer *ipsec-peer-name*

no ipsec peer *ipsec-peer-name*

Purpose

Applies IP Security (IPSec) transport mode encryption to the Layer 2 Tunneling Protocol (L2TP) tunnel.

Command Mode

L2TP configuration

Syntax Description

ipsec-peer-name	Name of the IPSec peer used to encrypt the L2TP packets.

Default

If this command is not used, the L2TP tunnel is not encrypted.

Usage Guidelines

Use the **ipsec peer** command to specify the name of the IPSec peer that is to be used to encrypt the L2TP tunnel. The IPSec peer named in this command must be associated with a proposal that uses transport encapsulation mode. See the **encapsulation-mode** command description in Chapter 27, "IPSec Commands" for more information.

Use the **no** form of this command to disassociate the IPSec peer from the L2TP peer.

Examples

The following example applies an IPSec peer called `corporate` to the L2TP peer being configured:

```
[local]RedBack(config-l2tp)#ipsec peer corporate
```

Related Commands

encapsulation-mode

l2tp-group name

l2tp-group name *group-name*

no l2tp-group name *group-name*

Purpose

Creates a group of Layer 2 Tunneling Protocol (L2TP) network servers (LNSs) among which Point-to-Point Protocol (PPP) sessions are parceled out. Also, enters L2TP group configuration mode.

Command Mode

context configuration

Syntax Description

group-name	Name of the L2TP group being created. L2TP group names must be unique from other L2TP group names, peer names, peer domain names, and group domain names.

Default

No L2TP group is created.

Usage Guidelines

Use the **l2tp-group name** command to create a group of L2TP LNSs among which PPP sessions are parceled out, and to enter L2TP group configuration mode. All LNSs in a group must be defined within the same context as the group itself. L2TP peers do not have to be defined prior to inclusion in a group and can be served by Remote Authentication Dial-In User Service (RADIUS). L2TP groups from RADIUS servers that support tunnel extensions (tunnel tags) are limited to 31 peers per group.

PPP sessions are distributed among peers according to the algorithm specified using the **algorithm** command in L2TP group configuration mode.

A group name created with the **l2tp-group name** command can be entered as the *tunnel-name* argument value for the following commands:

- **tunnel name** *tun-name* (subscriber configuration mode)
- **bind session** *tun-name context* (circuit configuration mode)

L2TP group names must be unique from other L2TP group names, names created using the **l2tp-peer name** command in context configuration mode, and names created using the **domain** command in both L2TP configuration and L2TP group configuration modes.

Use the **no** form of this command to disband the named group and delete all references to it by the L2TP peers that formed the group.

Examples

The following example creates an L2TP group called `group1`:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tpgrp)#
```

Related Commands

bind session
tunnel name
show l2tp group
show l2tp info

l2tp attribute calling-number real-circuit-id

l2tp attribute calling-number real-circuit-id

no l2tp attribute calling-number real-circuit-id

Purpose

Configures the L2TP access concentrator (LAC) to populate the contents of the Calling Number Attribute Value Pair (AVP) with the value of the Real Circuit ID AVP.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

The Calling Number AVP is not populated with the value of the Real Circuit ID AVP.

Usage Guidelines

Use the **l2tp attribute calling-number real-circuit-id** command to configure the LAC to populate the contents of the Calling Number AVP with the value of the Real Circuit ID AVP. This allows RADIUS servers to look in the Calling Number AVP for the Real Circuit ID information.

Use the **no** form of this command to disable population of the Calling Number AVP with the value of the Real circuit ID AVP.

Examples

The following example enables populating the Calling Number AVP with the value of the Real Circuit ID AVP:

```
[local]RedBack(config-ctx)#l2tp attribute calling-number real-circuit-id
```

Related Commands

show l2tp info

l2tp-peer default

l2tp-peer default [**local** *ipaddr*]

no l2tp-peer default

Purpose

Enters Layer 2 Tunneling Protocol (L2TP) configuration mode to change the factory default settings that are applied to new L2TP tunnel peers.

Command Mode

context configuration

Syntax Description

local *ipaddr*	Optional. Default local IP address to be used by new L2TP peers.

Default

L2TP tunnel peer default settings remain unchanged.

Usage Guidelines

Use the **l2tp-peer default** command to enter L2TP configuration mode for purposes of changing the default configuration for new L2TP peers. The configuration settings of individual peers override the new default settings, just as they would if the factory default settings remained unchanged.

Only one set of default settings can be configured per context. Once this new default configuration has been established, all new L2TP tunnel peers adopt the new settings, unless changed on an individual basis within the configuration of individual peers.

Use the **no** form of this command to return the default settings for new L2TP peers to the factory defaults.

Examples

The following example shows changing L2TP peer default settings from the factory defaults:

```
[local]RedBack(config-ctx)#l2tp-peer default
[local]RedBack(config-l2tp)#police rate 21000
[local]RedBack(config-l2tp)#retry 12
[local]RedBack(config-l2tp)#session-auth chap
```

Related Commands

show configuration

l2tp-peer name

l2tp-peer name *peer-name* **media** {**pvc** | **udp-ip remote** {**ip** *ipaddr* | **dns** *dns-name*} [**local** *ipaddr*]}

no l2tp-peer name *peer-name*

Purpose

Defines a Layer 2 Tunneling Protocol (L2TP) peer and enters L2TP configuration mode.

Command Mode

context configuration

Syntax Description

peer-name	Name of the L2TP tunnel peer. L2TP peer and group names must be unique from other peer names, group names, peer domain name, or group domain name. Within a context, L2TP peer names must also be unique from L2F peer and domain names.
media pvc	Specifies L2TP Asynchronous Transfer Mode (ATM) adaptation layer type 5 (AAL5) or L2TP Frame Relay, where the encapsulation is determined as part of the circuit definition.
media udp-ip	Specifies a User Datagram Protocol (UDP) IP-encapsulated tunnel.
remote ip *ipaddr*	Remote IP address. Required for UDP IP encapsulation.
remote dns *dns-name*	Remote Domain Name System (DNS) name.
local *ipaddr*	Optional. Local IP address.

Default

No L2TP peer is created.

Usage Guidelines

Use the **l2tp-peer name** command to define an L2TP peer and enter L2TP configuration mode. The name of the L2TP tunnel peer must be the same as the name that is provided by the peer as a hostname in Start-Control-Connection-Request (SCCRQ) packets. You can create an alias name for the tunnel with the **domain** command in L2TP configuration mode.

Tunnel peer names, group names, peer domain names, and group domain names must be unique. For example, if a peer is named john, no group, peer domain, or group domain can also be named john.

This command supports multiple L2TP tunnels that are identically named. This is commonly the case when Microsoft Windows clients are the L2TP peers.

Use the **no** form of this command to delete an existing L2TP tunnel peer.

Examples

The following example creates an L2TP-tunnel peer named `lac1.net`.

```
[local]RedBack(config-ctx)#l2tp-peer name lac1.net media pvc
[local]Redback(config-l2tp)#
```

Related Commands

domain
l2tp-peer unnamed
show l2tp info

l2tp-peer unnamed

l2tp-peer unnamed [**local** *ipaddr*]

no l2tp-peer unnamed

Purpose

Enters Layer 2 Tunneling Protocol (L2TP) configuration mode and configures support for anonymous tunnels.

Command Mode

context configuration

Syntax Description

local *ipaddr*	Optional. Default local IP address to be used by unnamed L2TP peers.

Default

Anonymous tunnel support is disabled.

Usage Guidelines

Use the **l2tp-peer unnamed** command to enter L2TP configuration mode and configure how the system responds to anonymous tunnels. Use the anonymous tunnel configuration for any incoming tunnel Start-Control-Connection-Request (SCCRQ) packets that contain a hostname not found in the local L2TP peer configurations or via Remote Authentication Dial-In User Service (RADIUS).

To configure the parameters of an anonymous L2TP tunnel, you can use all the L2TP configuration mode commands, except for **domain** and **static**. We recommend that you use the **tunnel-auth** command to accept all incoming tunnel requests that contain a specific tunnel password. In addition, although you can specify that L2TP access concentrator (LAC) and L2TP network server (LNS) support is enabled for an anonymous tunnel, we recommend that you restrict this to LNS using the **function lns-only** L2TP configuration mode command. Otherwise, outgoing calls might be placed on anonymous tunnels.

This command supports multiple L2TP tunnels that are identically named. This is commonly the case when Microsoft Windows clients are the L2TP peers.

Use the **no** form of this command to disable support for anonymous tunnels.

Examples

The following example enters L2TP configuration mode for purposes of configuring anonymous tunnel treatment:

```
[local]RedBack(config-ctx)#l2tp-peer unnamed
[local]Redback(config-l2tp)#
```

Related Commands

function
l2tp-peer name
show l2tp info
tunnel-auth

l2tp radius auto-group

l2tp radius auto-group

no l2tp radius auto-group

Purpose

Enable automatic creation of a tunnel group for multiple tunnels received in a Remote Authentication Dial-Up User Service (RADIUS) response.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

Automatic tunnel group creation is enabled.

Usage Guidelines

Use the **l2tp radius auto-group** command to enable automatic creation of a tunnel group for multiple tunnels (grouped by tags in accordance with RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*) received in a RADIUS response. This is the default behavior of SMS devices, so it is not necessary to enter this command unless the **no** form has previously been configured.

Use the **no** form of this command to override automatic tunnel group creation, allowing a RADIUS server to return a set of tunnels ordered by preference, using the Tunnel-Preference RADIUS attribute. The tunnel with the lowest preference value is attempted first. If tunnel creation fails, the system tries the tunnel with the next lowest preference value, and so on. This tunnel group override enables limited L2TP tunnel fail-over, and enables the RADIUS server to perform load-balancing of subscribers across tunnels.

To use the tunnel group override feature, the RADIUS server must respond with a full set of tunnel attributes, specifying client and server endpoints, and preference values grouped by tags.

In general, due to Point-to-Point Protocol (PPP) client timeouts and tunnel setup delay, we recommend returning no more than 3 tunnels in a RADIUS response.

The tunnel group override feature takes effect only if tunnel creation fails. If the tunnel is configured with a maximum session count, and the new PPP session would cause the maximum session count for the tunnel to be exceeded, the second tunnel is not be attempted.

Examples

The following example configures tunnel group override on the SMS device:

```
[local]RedBack(config)#no l2tp radius auto-group
```

Related Commands

None

l2x profile

l2x profile *prof-name*

no l2x profile *prof-name*

Purpose

Creates a Layer 2 Tunneling Protocol or Layer 2 Forwarding (L2X) tunnel profile and enters L2X profile configuration mode.

Command Mode

context configuration

Syntax Description

prof-name	Name of the tunnel profile to be created or modified.

Default

No L2X profile is created.

Usage Guidelines

Use the **l2x profile** command to create a new profile that can subsequently be applied to a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) peer. This command also enters L2X profile configuration mode. Once in L2X profile configuration mode, you can use the **min-subscribers** command to set the minimum number of subscriber slots that are to be reserved for all the peers (combined) to which the profile is assigned.

Use the **no** form of this command to delete the profile from the configuration.

Examples

The following example creates an L2X profile called `highest` and enters L2X profile configuration mode:

```
[local]RedBack(config-ctx)#l2x profile highest
[local]RedBack(config-l2xprof)#
```

The following example applies the L2X profile called `highest` to an L2TP peer called `proclean`:

```
[local]RedBack(config-ctx)#l2tp-peer name proclean media pvc
[local]RedBack(config-l2tp)#profile highest
```

See the **profile** command description in this chapter for more information on applying a profile to a peer.

Related Commands

min-subscribers
profile
show subscribers

l2tp eth-sess-idle-timeout

l2tp eth-sess-idle-timeout *seconds*

no l2tp eth-sess-idle-timeout

Purpose

Creates a session timeout specific to Ethernet traffic (does not consider Point-to-Point Protocol [PPP] traffic) that is triggered by the results of polling the session statistics.

Command Mode

global configuration

Syntax Description

seconds	Polling periods, in seconds. The range of values is 300 to 3,600.

Default

No timeout is configured.

Usage Guidelines

Use the **l2tp eth-sess-idle-timeout** command to configure a session timeout that is specific to Ethernet traffic (does not consider PPP traffic). The value of the *seconds* argument is the time between polls of the L2TP session statistics. If the inbound or outbound packet statistics show no change from the last poll, the session is considered idle and is terminated.

The timeout is typically configured in conjunction with using the **bridge-acl** *list-name* construct in the **bind session** command to filter packets so that only PPPoE traffic is allowed through an Ethernet over L2TP tunnel. If you configure the **l2tp eth-sess-idle-timeout** command, and you do not filter packets with a bridge access control list, any Ethernet traffic prevents the session from timing out.

If you have used the **debug l2x ses-setup** command to enable session setup debugging, a log message is displayed when a session times out.

Use the **no** form of this command to disable a previously configured timeout.

Examples

The following example sets the Ethernet timeout to `3000` seconds:

```
[local]RedBack(config)#l2tp eth-sess-idle-timeout 3000
```

Related Commands

bind session
debug l2x

local-name

local-name *hostname*

no local-name

Purpose

Sets the local hostname for an outbound Start-Control-Connection-Request (SCCRQ) control message.

Command Mode

L2TP configuration

Syntax Description

hostname	Local hostname.

Default

The system hostname as specified by the **system hostname** global configuration command is used as the local hostname.

Usage Guidelines

Use the **local-name** command when more than one tunnel, with different characteristics, are required for the same Layer 2 Tunneling Protocol (L2TP) peer.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to delete the specification of local hostname. To change a local hostname, create a new one and it overwrites the existing one.

Examples

The following example specifies the local hostname as `cardinal`:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#local-name cardinal
```

Related Commands

clear tunnel
system hostname

max-sessions

max-sessions *maxses*

no max-sessions

Purpose

Sets the maximum number of sessions allowed per tunnel for this Layer 2 Tunneling Protocol (L2TP) peer configuration.

Command Mode

L2TP configuration

Syntax Description

maxses	Maximum number of sessions allowed per tunnel. The range of values is 1 to 65,355; the default value is 65,355.

Default

The maximum number of sessions allowed per tunnel is the maximum number in the valid range (65,355).

Usage Guidelines

Use the **max-sessions** command to set the maximum number of sessions allowed per tunnel on the peer. For User Datagram Protocol (UDP) tunnels, a new tunnel opens if the *maxses* argument value has been reached for the current tunnel and the maximum number of tunnels (*maxtun* argument value for the **max-tunnels** command) has not been exceeded. For permanent virtual circuit (PVC) tunnels, because there can be only one tunnel per circuit, a new session is rejected if the *maxses* argument value has been reached.

Changing the configuration of a Layer 2 Tunneling Protocol (L2TP) peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

You cannot use this command if you entered L2TP configuration mode using the **l2tp-peer default** command.

Use the **no** form of this command to set the maximum number of sessions per tunnel to 65,355.

Examples

The following example sets the maximum number of sessions allowed per tunnel to `1000`:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#max-sessions 1000
```

Related Commands

clear tunnel
max-tunnels

max-tunnels

max-tunnels *maxtun*

no max-tunnels

Purpose

Sets the maximum number of tunnels allowed for the Layer 2 Tunneling Protocol (L2TP) peer.

Command Mode

L2TP configuration

Syntax Description

maxtun	Maximum number of tunnels allowed. The range of values is 1 to 128; the default value is 4.

Default

Four tunnels are allowed per peer.

Usage Guidelines

Use the **max-tunnels** command to set the maximum number of tunnels allowed for the peer. This command is only valid for User Datagram Protocol (UDP)-based tunnels; permanent virtual circuit (PVC)-based tunnels only allows one tunnel to be bound to an L2TP-encapsulated circuit.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to set the maximum number of tunnels allowed to 4.

Examples

The following example sets the maximum number of tunnels allowed to two:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#max-tunnels 2
```

Related Commands

clear tunnel
max-sessions

min-subscribers

min-subscribers *sub-num*

no min-subscribers

Purpose

Establishes a minimum number of subscriber slots to be reserved for the combined tunnel peers to which the Layer 2 Tunneling Protocol or Layer 2 Forwarding (L2X) profile is applied.

Command Mode

L2X profile configuration

Syntax Description

sub-num	Number of subscriber slots to be reserved.

Default

No subscriber slots are reserved.

Usage Guidelines

Use the **min-subscribers** command to set the minimum number of subscriber slots to be reserved for the peers to which the L2X profile is applied. All the peers to which the profile is applied share the minimum number of reserved subscriber slots specified by this command. If, for example, the profile specifies that a minimum of 1,200 subscriber slots are to be reserved, and the profile is applied to four peers, then the 1,200 subscribers slots are reserved for all four of those peers combined.

Use the **no** form of this command to remove the reserved minimum from the configuration of the profile.

Examples

The following example configures the profile named `apples` to have a minimum of `1500` reserved subscriber slots:

```
[local]RedBack(config-ctx)#l2x profile apples
[local]RedBack(config-l2xprof)#min-subscribers 1500
```

Related Commands

l2x profile
show subscribers

peer-name

peer-name *peer-name*

no peer-name *peer-name*

Purpose

Makes the named peer a member of the current Layer 2 Tunneling Protocol (L2TP) group.

Command Mode

L2TP group configuration

Syntax Description

name	Name of the peer to be added to the current L2TP group.

Default

No peer is added to the current L2TP group.

Usage Guidelines

Use the **peer-name** command to add a peer to an L2TP group. The *peer-name* argument can be either the peer name as indicated in the **l2tp-peer name** command, or any of the aliases for that peer created with the **domain** L2TP configuration mode command. When the redundancy algorithm is set to strict-priority using the **algorithm** command, the implicit priority is the order in which the **peer-name** commands are entered.

For Remote Authentication Dial-In User Service (RADIUS) configuration, the RADIUS attribute Tunnel-Preference specifies the relative priority of the individual peers, where lower numbers indicate higher priorities. See the **algorithm** command documentation for more information on RADIUS-based configuration of L2TP groups and the priorities of peer members.

This command takes effect immediately, but does not affect Point-to-Point Protocol (PPP) sessions that are already established, only future PPP sessions.

Changing the configuration of a peer group with established tunnels does not take effect until you delete all tunnels to the peers (using the **clear tunnel** command), or until all the tunnels to all the peers in the group come down naturally. The configuration database is queried again to reestablish tunnels to the peers, thereby implementing the new configuration.

Use the **no** form of this command to remove the named peer from the group.

Example

The following command selects (or creates) an L2TP group, adds three L2TP peers to the group, sets the algorithm to strict-priority, and sets the deadtime to five minutes:

```
[local]RedBack(config-ctx)#l2tp-group name group1
[local]RedBack(config-l2tpgrp)#peer-name sweet1
[local]RedBack(config-l2tpgrp)#peer-name sweet2
[local]RedBack(config-l2tpgrp)#peer-name sweet3
[local]RedBack(config-l2tpgrp)#algorithm first
[local]RedBack(config-l2tpgrp)#default deadtime
```

Related Commands

algorithm
clear tunnel
deadtime
description
domain
l2tp attribute calling-number real-circuit-id
l2tp-peer name
show l2tp info
show l2tp group

police

police rate *rate* **burst** *size*

no police

Purpose

Limits the aggregate packet stream received over a Layer 2 Tunneling Protocol (L2TP) tunnel by rate and burst tolerance.

Command Mode

L2TP configuration

Syntax Description

rate *rate*	Limiting rate in kbps. The range of values is 10 to 155,520 kbps.
burst *size*	Burst tolerance size in bytes. The range of values is 0 to 100,000 bytes.

Default

No limiting rate or burst tolerance is set.

Usage Guidelines

Use the **police** command to control incoming traffic. A general rule to determine burst tolerance is to multiply the link maximum transmission unit (MTU) by 10 (around 15,000 to 20,000 bytes for subscriber circuits). A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and burst tolerance are dropped.

If the value set by the **max-tunnels** command is greater than 1, the **rate-limit** command sets the rate for each tunnel. Only tunnels established after the **police** command has been entered are affected.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to remove any previously set rate or burst size limitations.

Examples

The following example sets limitations on the rate and burst size of incoming traffic through the tunnel:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#police rate 12 burst 17000
```

Related Commands

clear tunnel
max-tunnels
rate-limit

profile

profile *prof-name*

no profile *prof-name*

Purpose

Applies a Layer 2 Tunneling Protocol or Layer 2 Forwarding (L2X) tunnel profile to a Layer 2 Tunneling Protocol (L2TP) peer.

Command Mode

L2TP configuration

Syntax Description

prof-name	Name of the tunnel profile to be applied to the peer.

Default

No L2X profile is applied to the L2TP peer.

Usage Guidelines

Use the **profile** command to apply an L2X tunnel profile to an L2TP peer. All the peers to which the profile is applied share the minimum number of reserved subscriber slots specified in the configuration of the profile. If, for example, the profile specifies that a minimum of 1,200 subscriber slots are to be reserved, and the profile is applied to four peers, then the 1,200 subscribers slots are reserved for all four of those peers combined.

You can apply a profile to L2TP and Layer 2 Forwarding (L2F) peers, and you can configure multiple profiles in a context. The total number of reserved subscriber slots designated in a context's profiles cannot exceed the number reserved for the context as a whole using the **aaa min-subscribers** command. However, it is not necessary to have the **aaa min-subscribers** command in the configuration to reserve subscriber slots for tunnel peers using the **profile** command.

Use the **no** form of this command to disassociate the peer from the profile.

Examples

The following example applies an L2X profile called `highest` to an L2TP peer called `proclean`:

```
[local]RedBack(config-ctx)#l2tp-peer name proclean media pvc
[local]RedBack(config-l2tp)#profile highest
```

Related Commands

aaa min-subscribers
l2x profile
min-subscribers
show subscribers

rate-limit

rate-limit rate *rate* **burst** *size*

no rate-limit

Purpose

Limits the aggregate packet stream transmitted over a Layer 2 Tunneling Protocol (L2TP) tunnel by rate and burst tolerance.

Command Mode

L2TP configuration

Syntax Description

rate *rate*	Limiting rate in kbps. The range of values is 10 to 155,520 kbps.
burst *size*	Burst tolerance size in bytes. The range of values is 0 to 100,000 bytes.

Default

There is no limitation on the rate and burst size of outgoing traffic.

Usage Guidelines

Use the **rate-limit** command to control outgoing traffic. A general rule to determine burst tolerance is to multiply the link maximum transmission unit (MTU) by 10 (around 15,000 to 20,000 bytes for subscriber circuits). A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and burst tolerance are dropped.

If the **max-tunnels** value is greater than 1, the **rate-limit** command sets the rate for each tunnel. Only tunnels established after the **rate-limit** command has been entered are affected.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to remove any previously set limitation.

Examples

The following example sets limitations on the rate limit and burst size of outgoing traffic through the tunnel:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#rate-limit rate 12 burst 17000
```

Related Commands

clear tunnel
max-tunnels
police

retry

retry *count*

default retry

Purpose

Sets the number of times an unacknowledged control message is retransmitted to a Layer 2 Tunneling Protocol (L2TP) peer before the tunnel is brought down.

Command Mode

L2TP configuration

Syntax Description

count	Number of times an unacknowledged control message is retransmitted to a peer. The range of values is 1 to 255; the default value is 5.

Default

An unacknowledged control message is retransmitted five times.

Usage Guidelines

Use the **retry** command to set the number of times an unacknowledged control message is retransmitted to a peer before the tunnel is brought down. You may want to increase the value from the default of 5 if the L2TP media is not reliable.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to set the number of retranmissions to five.

Examples

The following example configures the peer so that unacknowledged control messages are retransmitted six times before the tunnel is brought down:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#retry 5
```

Related Commands

clear tunnel
timeout
tunnel-window

secondary-tunnel-auth

secondary-tunnel-auth *secret*

no secondary-tunnel-auth *secret*

Purpose

Sets a secondary Layer 2 Tunneling Protocol (L2TP) password to the tunnel peer.

Command Mode

L2TP configuration

Syntax Description

secret	Secondary L2TP password for the tunnel. The password can be any alphanumeric text string of any length.

Default

No secondary password is created.

Usage Guidelines

Use the **secondary-tunnel-auth** command to set the secondary L2TP password to the tunnel peer. The secondary password is only used on an L2TP access concentrator (LAC) that initiates a connection, and only if the primary password (set by the **tunnel-auth** command) fails. Although an L2TP network server (LNS) can also initiate a connection, the secondary password feature is not supported in that case.

The typical use for the secondary password feature is to facilitate a transition from an old password to a new one. You can change the password on the LAC side of an L2TP tunnel without first notifying LNSs and other LACs.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to delete any previously established secondary password.

Examples

The following example establishes `reet4493ek` as the secondary L2TP peer password:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#secondary-tunnel-auth reet4493ek
```

Related Commands

clear tunnel
l2tp-peer name
tunnel-auth

session-auth

session-auth {**pap** | **chap** | **chap pap**} [**context** *ctx-name* | **service-group** *group-name*]

default session-auth

Purpose

Specifies the method used by a Layer 2 Tunneling Protocol (L2TP) network server (LNS) to authenticate subscriber sessions that arrive over this tunnel.

Command Mode

L2TP configuration

Syntax Description

pap	Specifies that Password Authentication Protocol (PAP) is to be used to obtain the username and password from the subscriber.
chap	Specifies that Challenge Handshake Authentication Protocol (CHAP) is to be used to obtain the username and password from the subscriber.
chap pap	Specifies that either CHAP or PAP can be used to obtain the username and password from the subscriber, but that CHAP is preferred.
context *ctx-name*	Optional. Name of a specific context to which subscriber sessions are restricted.
service-group *group-name*	Optional. Name of a service access list that limits the services available to the circuit or port.

Default

CHAP or PAP can be used as an authentication method.

Usage Guidelines

Use the **session-auth** command to specify the method used by an L2TP LNS to authenticate subscriber sessions that arrive over the tunnel. If dialed number information string (DNIS)-based tunnel selection has been specified for the peer using the **dnis only** command, the **session-auth** command is ignored.

Use the optional **context** *ctx-name* construct to prevent dynamic context selection, thereby limiting the services available to any PPP sessions that arrive from this peer. Specifically, these sessions are limited to terminating and routing in the named context and to entering a tunnel defined within that context. If the **context** *ctx-name* construct is present, the Access Operating System (AOS) attempts to authenticate the session according to the authentication, authorization, and accounting (AAA) configuration for the named context, rather than according to the context portion of the structured username, if present. If the user passes

authentication, the session comes up. If Remote Authentication Dial-In User Service (RADIUS) returns a Context-Name attribute whose value conflicts with the **context** *ctx-name* construct (or any of its aliases) in the command line, the binding fails. Authentication also fails if global authentication is configured and the Access-Response packet from the RADIUS server does not contain a Context-Name attribute.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to set the LNS to use CHAP PAP to authenticate subscriber sessions.

Examples

The following example establishes that either PAP or CHAP can be used to authenticate subscriber sessions:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#session-auth pap
```

Related Commands

clear tunnel
dnis
function

show l2tp counters

show l2tp counters [**disconnect-reasons** | [**peer** *peer-name* [**tunnel** *tunnel-id* [**session** *session-id*]]]]

Purpose

Displays the statistics for Layer 2 Tunneling Protocol (L2TP) tunnels.

Command Mode

operator exec

Syntax Description

disconnect-reasons	Optional. Displays connection disconnect notification (CDN) reasons reported by any peers in the context.
peer *peer-name*	Optional. Name of the peer for which you want detailed information displayed.
tunnel *tunnel-id*	Optional when you use the **peer** *peer-name* construct. Tunnel number of the tunnel for which you want detailed information displayed.
session *session-id*	Optional when you use the **peer** *peer-name* and **tunnel** *tunnel-id* constructs. Session number of the session for which you want detailed information displayed.

Default

Displays information for all peers in the current context.

Usage Guidelines

Use the **show l2tp counters** command without any optional constructs to see the L2TP tunnel counters shown in Table 25-1 for each L2TP peer.

Table 25-1 Output When No Optional Constructs are Used

Field	Description
Tx Pkts	Number of packets transmitted
Rx Pkts	Number of packets received
Tunnels Count	Number of tunnels bound to this peer in any state
Errs	Total number of control message errors (each tunnel has one control channel)

Table 25-1 Output When No Optional Constructs are Used

Field	Description
Sessions Count	Total number of sessions to the peer in any state
Sessions disconnected by peer	Number of sessions disconnected by each peer
Tunnel failures (retries exceeded)	Number of tunnel failures due to unsuccessful retries

Use the optional **disconnect-reasons** keyword to display the counters shown in Table 25-2.

Table 25-2 Output When disconnect-reasons Key Word is Used

Field	Description
Unspecified	Number of disconnects for unspecified reasons
Loss of carrier	Number of disconnects due to loss of carrier
Administrative	Number of disconnects for administrative reasons
Temporary Resources	Number of disconnects due to shortage of temporary resources
Permanent Resources	Number of disconnects due to shortage of permanent resources
Invalid destination	Number of disconnects due to invalid destination specification
No carrier detected	Number of disconnects due to no carrier being detected
Busy signal detected	Number of disconnects due to busy signal
No dial tone	Number of disconnects due to no dial tone being detected
Timeout	Number of disconnects due to timeout
Framing error	Number of disconnects due to framing errors
General Errors: None	Number of general errors
General Errors: No control connection	Number of disconnects due to control connection being missing
General Errors: Bad Length	Number of disconnects due to invalid length of packets
General Errors: Invalid Value	Number of disconnects due to invalid data values
General Errors: Insufficient Resources	Number of disconnects due to insufficient resources
General Errors: Invalid Session ID	Number of disconnects due to invalid session ID
General Errors: Unspecified	Number of disconnects for unspecified reasons
General Errors: Wrong LNS	Number of disconnects due to incorrect LNS specification
General Errors: Unknown AVP	Number of disconnects due to invalid AVP specification
Other	Number of errors not included under any other heading

Use the optional **peer** *peer-name* construct to display the counters shown in Table 25-3.

Table 25-3 Output When a Specific Peer is Named

Field	Description
Tx Data Packets	Number of data packets transmitted by the peer
Rx Data Packets	Number of data packets received by the peer
Tx Data Bytes	Number of data bytes transmitted by the peer
Rx Data Bytes	Number of data bytes received by the peer
Tx Control Packets	Number of control packets transmitted by the peer
Rx Control Packets	Number of control packets received by the peer
Tx Control Bytes	Number of control bytes transmitted by the peer
Rx Control Bytes	Number of control bytes received by the peer
Police pkts drops	Number of packets dropped due to policing constraints
Rate pkts drops	Number of packets dropped due to rate limiting constraints
Tx SCCRQ Count	Number of Start-Control-Connection-Request (SCCRQ) messages transmitted by the peer
Rx SCCRQ Count	Number of SCCRQ messages received by the peer
Active Tunnels	Number of tunnels bound to the peer that are in the up state
Tunnel Ctl Errors	Number of control errors on the peer—cumulative for all current tunnels (in any state)
Session Count	Number of sessions in the peer—cumulative for all current tunnels (in any state)
Tunnel Data Errors	Number of data errors logged—cumulative for all current tunnels (in any state)
Rem ID	For each tunnel in the peer, the remote peer's tunnel ID
Session Cnt	For each tunnel in the peer, the number of sessions in any state
Tx Pkts	For each tunnel in the peer, the number of packets transmitted
Rx Pkts	For each tunnel in the peer, the number of packets received
State	For each tunnel in the peer, the current state

Use the optional **tunnel** *tunnel-id* construct to display the counters shown in Table 25-4.

Table 25-4 Output When a Specific Peer and Tunnel are Named

Field	Description
Tx Data Packets	Number of data packets transmitted through the tunnel
Rx Data Packets	Number of data packets received through the tunnel
Tx Data Bytes	Number of data bytes transmitted through the tunnel
Rx Data Bytes	Number of data bytes received through the tunnel

Table 25-4 Output When a Specific Peer and Tunnel are Named

Field	Description
Tx Control Packets	Number of control packets transmitted through the tunnel
Rx Control Packets	Number of control packets received through the tunnel
Tx Control Bytes	Number of control bytes transmitted through the tunnel
Rx Control Bytes	Number of control bytes received through the tunnel
Police pkts drops	Number of packets dropped due to policing constraints
Rate pkts drops	Number of packets dropped due to rate-limiting constraints
Tunnel Ctl Errors	Number of tunnel control errors—cumulative for all current tunnels (in any state)
Last Ctl Error	Name of the last control error logged
Last Ctl Err Time	Time the last control error was logged
Tunnel Data Errors	Number of tunnel data errors—cumulative for all current tunnels (in any state)
Last Data Error	Name of the last data error logged
Last Data Err Time	Time the last data error was logged
Tx SCCRQ Count	Number of SCCRQ messages transmitted through the tunnel
Tx Last SCCRQ Time	Time the last SCCRQ message was transmitted through the tunnel
Tx Last SCCCN Time	Time the last Start-Control-Connection-Connected (SCCCN) message was transmitted through the tunnel
Rx SCCRQ Count	Number of SCCRQ messages received through the tunnel
Rx Last SCCRQ Time	Time the last SCCRQ message was received through the tunnel
Rx Last SCCCN Time	Time the last SCCCN message was received through the tunnel
Session Count	Number of sessions (in any state) in the tunnel
Active Sessions	Number of sessions in the established state in the tunnel
Total Act Sessions	Number of sessions that reached the established state in this tunnel—cumulative since the tunnel came up
Total Fail Session	Number of sessions that failed to reach the established state in this tunnel - cumulative since the tunnel came up
Ses ID	For each session on the tunnel, the local session ID
Rem ID	For each session on the tunnel, the remote session ID
Type	For each session on the tunnel, whether the session is acting as a LAC or an LNS
Tx Pkts	For each session on the tunnel, the number of packets transmitted
Rx Pkts	For each session on the tunnel, the number of packets received
State	The state of each session on the tunnel
PPP Subscriber	Can contain (ETHERNET) to indicate an Ethernet-encapsulated session. (NO SUBSCRIBER) can appear for a dialed number information string (DNIS)-based tunnel switch on an L2TP network server (LNS) session. A bind session can only occur on a real L2TP access concentrator (LAC).

Use the optional **session** *session-id* construct to display the counters shown in Table 25-5.

Table 25-5 Output When a Specific Peer, Tunnel, and Session are Named

Field	Description
Tx Data Packets	Number of data packets transmitted during the session
Rx Data Packets	Number of data packets received during the session
Tx Data Bytes	Number of data bytes transmitted during the session
Rx Data Bytes	Number of data bytes received during the session

Examples

The following example displays the output for the **show l2tp counters** command when no optional constructs are used:

```
[local]RedBack>show l2tp counters

Tunnels        Sessions
Peer Name      Tx Pkts  Rx Pkts    Count Errs  Count Active   Failed
-----------    -------- ---------- ----- ----- ----- -------- ---------
lac3           6        6          1     0     1     1        0
lns3.net       6        6          1     0     1     1        0

Sessions disconnected by peer:      0
Tunnel Failures (retries exceeded): 0
```

The following example displays the output for the **show l2tp counters** command when the **disconnect-reasons** keyword is used:

```
[local]RedBack>show l2tp counters disconnect-reasons

Unspecified:           405450264   General Errors:
Loss of Carrier:       405450424     None:                    13
Administrative:        405452888     No Control Connection:   8192
Temporary Resources:   405450896     Bad Length:              16383
Permanent Resources:   405450696     Invalid Value:           406275488
Invalid Destination:   405209600     Insufficient Resources:  406275488
No Carrier Detected:   405432984     Invalid Session ID:      405650976
Busy Signal:           15          Unspecified:               405458740
No Dial Tone:          405433768      Wrong LNS:              12886320
Timeout:               405433720      Unknown AVP:            1
Framing Error:         405433672
Other:                 1

Total:                 -240768368
```

The following example displays the output for the **show l2tp counters** command when a specific peer is named:

```
[local]RedBack>show l2tp counters peer lac

Tx Data Packets:             6          Rx Data Packets:             6
Tx Data Bytes:             126          Rx Data Bytes:             147
Tx Control Packets:          5          Rx Control Packets:          4
Tx Control Bytes:          188          Rx Control Bytes:          286
Police pkts drops:           0          Rate pkts drops:             0
Tx SCCRQ Count:              0          Rx SCCRQ Count:              1


Active Tunnels:          1              Tunnel Ctl Errors:      0
Session Count:           1              Tunnel Data Errors:     0

                 Rem   Ses
Tunnel Name      ID    Cnt   Tx Pkts    Rx Pkts    State
---------------- ----- ----- ---------- ---------- ---------------
lac3:1           1     1     6          6          ESTABLISHED
```

The following example displays the output for the **show l2tp counters** command when a specific peer and a specific tunnel are named. Each of the first three sessions is bound with the **bind session** command.

```
[local]RedBack>show l2tp counters peer lac tunnel 1

Tx Data Packets:             6          Rx Data Packets:             6
Tx Data Bytes:             126          Rx Data Bytes:             147
Tx Control Packets:          6          Rx Control Packets:          5
Tx Control Bytes:          208          Rx Control Bytes:          298
Police pkts drops:           0          Rate pkts drops:             0


Tunnel Ctl Errors:           0
Last Ctl Error:          (NONE)
Last Ctl Err Time:    (NO TIME)


Tunnel Data Errors:          0
Last Data Error:             0
Last Data Err Time:   (NO TIME)


Tx SCCRQ Count:              0
Tx Last SCCRQ Time: (NO TIME)
Tx Last SCCCN Time: (NO TIME)


Rx SCCRQ Count:              1
Rx Last SCCRQ Time: MON JUN 11 18:03:16 2001
Rx Last SCCCN Time: MON JUN 11 18:03:16 2001
```

```
Session Count:          1          Active Sessions:             1
Total Act Sessions:     1          Total Fail Session:          0

 Ses   Rem
 ID    ID   Type Tx Pkts    Rx Pkts    State       PPP Subscriber
----- ----- ---- ---------- ---------- ----------- --------------------
 2     2    LNS  6          6          ESTABLISHED client3@lns3.net
```

Related Commands

l2tp-peer name
show l2tp info

show l2tp group

show l2tp group [*group-name*]

Purpose

Displays Layer 2 Tunneling Protocol (L2TP) group configuration information.

Command Mode

operator exec

Syntax Description

group-name	Optional. Name of an L2TP group to be displayed.

Default

Displays all L2TP groups in the current context.

Usage Guidelines

Use the **show l2tp group** command to view the redundancy algorithm and deadtime of one specific L2TP group or for all groups in the current context. When you display information for a specific group, the names of the peer members of the group and information about each peer are also displayed (see examples).

Examples

The following example shows using the **show l2tp group** command to display a particular group (called `l2tp`). The asterisk (*) in front of the peer called `l2tp_1` indicates that the peer is dead (see the **deadtime** L2TP group configuration mode command for more information on this status).

```
[local]RedBack>show l2tp group l2tp

Group name:      l2tp  RADIUS:  YES
Algorithm        Load-balance  Deadtime: 10

Peers:           pvc_l2tp              *l2tp_1
                 l2tp_2

Domains: vpn
```

```
                              Max  Tun    Max   Ses
Peer Name  Local Name Med   Tuns  Cnt    Ses   Cnt  Stat  LAC  LNS  Named
---------- ----------  ---   ----  ---   ---   ---- ----  ---  ---  -----
pvc_l2tp    tgrp3      PVC   1     1    65535  7    NO    YES  YES   YES
l2tp_1      tgrp1      UDP    1     0   20     0    NO    YES  YES   YES
l2tp_2      tgrp2      UDP    1     1   65535  6    NO    YES  YES   YES
```

The following example shows the result when you use the **show l2tp group** command without specifying a group name:

```
[local]RedBack>show l2tp group

Group Name       Algorithm    Deadtime
---------------- ------------ --------
l2tp             Load-balance 10
l2tp2            Load-balance 5
l2tp3            Load-balance 10
```

Related Commands

clear tunnel
deadtime
l2tp attribute calling-number real-circuit-id
show l2tp info

show l2tp info

show l2tp info [**peer** *peer-name* [**tunnel** *tunnel-id* [**session** *session-id*]]]

Purpose

Displays a summary of status and configuration for Layer 2 Tunneling Protocol (L2TP) tunnels.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Optional. Name of the peer for which you want detailed information displayed.
tunnel *tunnel-id*	Optional if you use the **peer** *peer-name* construct. Tunnel number of the tunnel for which you want detailed information displayed.
session *session-id*	Optional if you use the **tunnel** *tunnel-id* construct. Session number of the session for which you want detailed information displayed.

Default

Displays all peers in the current context.

Usage Guidelines

Use the **show l2tp info** command without any optional constructs to see the L2TP tunnel information shown in Table 25-6 for each L2TP peer:

Table 25-6 Output When No Optional Constructs are Used

Field	Description
Local Name	Local hostname for outbound Start-Control-Connection-Request (SCCRQ) control messages
Med	Media—tunnel encapsulation type (permanent virtual circuit [PVC] or User Datagram Protocol [UDP])
Max Tuns	Maximum number of tunnels allowed on the peer
Tun Cnt	Number of tunnels (in any state) to the peer
Max Ses	Maximum number of sessions allowed per tunnel
Ses Cnt	Number of sessions (in any state) for the peer

Table 25-6 Output When No Optional Constructs are Used

Field	Description
Stat	Whether one tunnel is maintained to the peer at all times (Stat = YES) or tunnels are established on demand (Stat = NO)
Mode	L2TP access concentrator (LAC), L2TP network server (LNS), or LAC and LNS
Named	Whether the peer is named (Named = YES) or unnamed (Named = NO)

Use the optional **peer** *peer-name* construct to display the information shown in Table 25-7.

Table 25-7 Output When a Specific Peer is Named

Field	Description
Peer name	Name of the peer you specified.
Media	Tunnel encapsulation type (PVC or UDP).
Hostname alias	Local hostname for outbound SCCRQ control messages.
RADIUS	Whether the peer is served by the Remote Authentication Dial-In User Service (RADIUS).
Configured Rem IP	Remote IP address of the peer as entered in the **l2tp-peer name** command.
Static	Whether one tunnel is maintained to the peer at all times (Static = YES) or tunnels are established on demand (Static = NO).
Local IP address	Local IP address of the peer as entered in the **l2tp-peer name** command.
Unnamed	Whether the peer is unnamed (Unnamed = YES) or named (Unnamed = NO). If Unnamed=YES, the peer name displayed was automatically obtained from the remote host name contained in the incoming SCCRQ.
LAC	Whether the peer has LAC functionality.
Maximum Tunnels	Maximum number of tunnels allowed on the peer.
LNS	Whether the peer has LNS functionality.
Maximum Ses/Tunnel	Maximum number of sessions allowed per tunnel.
Ctl retran timeout	Number of seconds to wait for an acknowledgment before a control message is retransmitted.
Ctl retran count	Number of control message retransmissions.
Session auth	Method used to authenticate subscriber sessions. Applies only to Point-to-Point Protocol (PPP) over L2TP sessions. Meaningful at the LNS only.
Control window	Number of control messages the peer can send without acknowledgment from the Subscriber Management System (SMS) device.
DNIS	Whether dialed number information string (DNIS)-based tunnel switching is enabled.
DNIS ONLY	Whether DNIS attribute must be present on incoming session for the sessions to be accepted.

Table 25-7 Output When a Specific Peer is Named

Field	Description
Police rate	Limiting rate on incoming traffic.
Police burst	Burst rate on incoming traffic.
Rate-limit rate	Limiting rate on outgoing traffic.
Rate-limit burst	Burst rate on outgoing traffic.
Group	Name of the L2TP group (if any) to which the peer belongs.
Preference	Load-balancing preference of the peer within its group. Not valid if the peer is not a member of an L2TP group.
Tunnel password	L2TP tunnel password for tunnel authentication.
Session context	Context (if any) to which sessions are restricted. Applies only to PPP over L2TP sessions. Meaningful at the LNS only.
Session service	Service group (if any) to which services available are limited. Applies only to PPP over L2TP sessions. Meaningful at the LNS only.
Ethernet encap	Type of Ethernet encapsulation to be used for any Ethernet sessions on the peer.
Ethernet session	Authentication or binding method to be used for any Ethernet sessions on the peer.
Domains	Peer aliases created with the **domain** command.
Tunnel Count	Number of tunnels (any state) on the peer.
Tunnel Ctl Errors	Number of tunnel control errors.
Session Count	Number of sessions (any state) on the peer, all tunnels combined.
Tunnel Data Errors	Number of tunnel data errors.
Tunnel Name	Name of each tunnel to the peer followed by a local ID.
Rem ID	For each tunnel, the remote tunnel ID.
Ses Cnt	For each tunnel, the number of sessions in any state.
Cntl Errs	For each tunnel, the number of control errors logged.
Last Err	For each tunnel, the name of the last error logged.
Remote IP/PVC	For each tunnel, the remote IP address or PVC (for example, slot.port.vpi.vci or slot.port.dlci) over which the PVC media tunnel is established.
State	For each tunnel, the operational state.

Use the optional **tunnel** *tunnel-id* construct to show the information shown in Table 25-8.

Table 25-8 Output When a Specific Peer and Tunnel are Named

Field	Description
Peer name	Name of the peer you specified.
Media	Tunnel encapsulation type (PVC or User Datagram Protocol [UDP]).

Table 25-8 Output When a Specific Peer and Tunnel are Named

Field	Description
Hostname alias	Local hostname for outbound SCCRQ control messages.
RADIUS	Whether the peer is served by RADIUS.
Remote IP address	Remote IP address of the peer as sent by the peer. May be different from the remote IP address configured with the **l2tp-peer name** command. This address is only used by the SMS device if the SMS device initialized the session (for security reasons). If the session was initialized by the remote peer, the configured remote IP address is used instead.
Static	Whether one tunnel is maintained to the peer at all times (Static = YES) or tunnels are established on demand (Static = NO).
Local IP address	Local IP address of the peer as entered in the **l2tp-peer name** command.
Unnamed	Whether the peer is unnamed (Unnamed = YES) or named (Unnamed = NO). If Unnamed=YES, the peer name displayed was automatically obtained from the remote hostname contained in the incoming SCCRQ.
LAC	Whether the peer has LAC functionality.
Maximum Tunnels	Maximum number of tunnels allowed on the peer.
LNS	Whether the peer has LNS functionality.
Maximum Ses/Tunnel	Maximum number of sessions allowed per tunnel.
Ctl retran timeout	Number of seconds to wait for an acknowledgment before a control message is retransmitted.
Ctl retran count	Number of control message retransmissions.
Session auth	Method used to authenticate subscriber sessions. Applies only to PPP over L2TP sessions. Meaningful at the LNS only.
Control window	Number of control messages the peer can send without acknowledgment from the SMS device.
DNIS	Whether DNIS-based tunnel switching is enabled.
DNIS ONLY	Whether the DNIS attribute must be present on incoming sessions for the sessions to be accepted.
Police rate	Limiting rate on incoming traffic.
Police burst	Burst rate on incoming traffic.
Rate-limit rate	Limiting rate on outgoing traffic.
Rate-limit burst	Burst rate on outgoing traffic.
Group	Name of the L2TP group (if any) to which the peer belongs.
Preference	Load-balancing preference of the peer within its group. Not valid if the peer is not a member of an L2TP group.
Tunnel password	L2TP tunnel password for tunnel authentication.
Session context	Context (if any) to which sessions are restricted. Applies only to PPP over L2TP sessions. Meaningful at the LNS only.
Session service	Service group (if any) to which services available are limited. Applies only to PPP over L2TP session. Meaningful at the LNS only.

Table 25-8 Output When a Specific Peer and Tunnel are Named

Field	Description
Ethernet encap	Type of Ethernet encapsulation to be used for any Ethernet sessions on the peer.
Ethernet session	Authentication or binding method to be used for any Ethernet sessions on the peer.
Domains	Peer aliases created with the **domain** command.
State	Operational state of the tunnel.
Tunnel Ctl Errors	Number of control errors logged for the tunnel.
Last Ctl Error	Name of the last control error logged for the tunnel.
Last Ctl Time	Time the last control error for the tunnel was logged.
Tunnel Data Errors	Number of data errors logged for the tunnel.
Last Data Error	Name of the last data error logged for the tunnel.
Last Data Err Time	Time the last data error for the tunnel was logged.
Session Count	Number of sessions (in any state) in the tunnel.
Active Sessions	Number of sessions in the established state in the tunnel.
Total Act Sessions	Number of sessions that reached the established state in this tunnel - cumulative since the tunnel came up.
Total Fail Session	Number of sessions that failed to reach the established state in this tunnel—cumulative since the tunnel came up.
Ses ID	For each session on the tunnel, the local session ID.
Rem ID	For each session on the tunnel, the remote session ID.
Type	For each session on the tunnel, whether the local session is acting as a LAC or an LNS.
State	State of each session on the tunnel.
PPP Subscriber	Can contain (ETHERNET) to indicate an Ethernet-encapsulated session. Can contain (NO SUBSCRIBER) for a DNIS-based tunnel switch on an LNS session. A bind session can only occur on a real LAC.
Tunnel Switching: Context	Contains the context name for the tunnel to which the session is tunnel-switched. This field is blank if the session is not tunnel-switched.
Tunnel Switching: Tunnel	Contains the tunnel name for the tunnel to which the session is tunnel-switched. This field is blank if the session is not tunnel-switched.

Use the optional **session** *session-id* construct to display the information shown in Table 25-9.

Table 25-9 Output When a Specific Peer, Tunnel, and Session are Named

Field	Description
Tx Data Packets	Number of data packets transmitted during the session
Rx Data Packets	Number of data packets received during the session

Table 25-9 Output When a Specific Peer, Tunnel, and Session are Named

Field	Description
Tx Data Bytes	Number of data bytes transmitted during the session
Rx Data Bytes	Number of data bytes received during the session

Examples

The following example shows output for the **show l2tp info** command when used without any optional constructs:

```
[local]RedBack>show l2tp info

                              Max  Tun  Max Ses
Peer Name  Local Name  Med    Tuns Cnt  Ses Cnt Stat  Mode  Named
---------  ----------- ----   ---- ---  --- ---- ---  ---   ----
l2tp_1     tgrpl       UDP    1    1    20   20  NO   YES   YES
l2tp_2     tgrp2       UDP    1    1    20   20  NO   YES   YES
pvc_l2tp   tgrp3       PVC    1    1   65535 20  NO   YES   YES
```

The following example shows output for the **show l2tp info** command when a specific peer is named:

```
[local]RedBack>show l2tp info peer l2tp_1

Peer name:          l2tp_1        Media:              UDP
Hostname alias:     tgrp1         RADIUS:             YES
Configured Rem IP:  11.1.1.2      Static:             NO
Local IP address:   11.1.1.1      Unnamed:            NO
LAC:                YES           Maximum Tunnels:    1
LNS:                YES           Maximum Ses/Tunnel: 20
Ctl retran timeout: 4             Ctl retran count:   3
Session auth:       CHAP          PAP Control window: 10
DNIS:               NO            DNIS ONLY:          NO
Police rate:        0             Police burst:       0
Rate-limit rate:    0             Rate-limit burst:   0
Group:              l2tp          Preference:         1
Tunnel password:    jiffy
Session context:    (NO CONTEXT)  Session Service:    (NO SERV GRP)
Ethernet encap:     None
Ethernet session:
Domains:            vpn_1

Tunnel Count:       1             Tunnel Ctl Errors:  41
Session Count:      20            Tunnel Data Errors: 0

             Rem   Ses   Cntl  Last
Tunnel Name  ID    Cnt   Errs  Err     Remote IP / PVC  State
-----------  ----  ---   ----  ------- ---------------- --------
l2tp:1        1     20    41   REXMT   11.1.1.2        ESTABLISHED
```

The following example shows output for the **show l2tp info** command when a specific peer and tunnel are named. Session 2 in this example is Ethernet over L2TP. The remote IP address is different from the configured remote IP address shown in the previous example. The remote IP address displayed when a specific tunnel is named is the address sent by the remote peer and may be different from the address configured with the **l2tp-peer name** command. The SMS device only uses the remote address sent by the peer if the SMS device initialized the session (for security reasons).

```
[local]RedBack>show l2tp info peer lns tunnel 1

Peer name:          lns           Media:              UDP
Hostname alias:     lac           RADIUS:             NO
Remote IP address:  10.1.1.2      Static:             NO
Local IP address:   11.1.1.1      Unnamed:            NO
LAC:                YES           Maximum Tunnels:    1
LNS:                YES           Maximum Ses/Tunnel: 65535
Ctl retran timeout: 4             Ctl retran count:   3
Session auth:       CHAP PAP      Control window:     10
DNIS:               NO            DNIS ONLY:          NO
Police rate:        0             Police burst:       0
Rate-limit rate:    0             Rate-limit burst:   0
Group:              (NO GROUP)    Preference:         0
Tunnel password:    (NO PASSWORD)
Session context:    (NO CONTEXT)  Session service: (NO SERVICE GROUP)
Ethernet encap:     NONE
Ethernet session:
Domains:            l2tp

State: ESTABLISHED

Tunnel Ctl Errors:  41
Last Ctl Error:     REM_WNDOFUL
Last Ctl Err Time:  TUE OCT 05 10:00:10 1999

Tunnel Data Errors: 0
Last Data Error:    0
Last Data Err Time: (NO TIME)

Session Count:       20           Active Sessions: 20
Total Act Sessions: 20            Total Fail Session: 0

Ses Rem                            Tunnel  Switching
ID  ID Type State PPP   Subscriber Context Tunnel
--- -- ---- ----- ---   ---------- ----------------
2   2  LAC  ESTABLISHED (ETHERNET)
3   3  LAC  ESTABLISHED joe32@l2tp
4   4  LAC  ESTABLISHED joe33@l2tp
5   5  LAC  ESTABLISHED joe34@l2tp
6   6  LAC  ESTABLISHED joe35@l2tp
7   7  LAC  ESTABLISHED joe36@l2tp
8   8  LAC  ESTABLISHED joe37@l2tp
9   9  LAC  ESTABLISHED joe38@l2tp
10  10 LAC  ESTABLISHED joe39@l2tp
```

```
11  11 LAC  ESTABLISHED joe40@l2tp
12  12 LAC  ESTABLISHED joe41@l2tp
13  13 LAC  ESTABLISHED joe42@l2tp
14  14 LAC  ESTABLISHED joe43@l2tp
15  15 LAC  ESTABLISHED joe44@l2tp
16  16 LAC  ESTABLISHED joe45@l2tp
17  17 LAC  ESTABLISHED joe46@l2tp
18  18 LAC  ESTABLISHED joe47@l2tp
19  19 LAC  ESTABLISHED joe48@l2tp
20  20 LAC  ESTABLISHED joe49@l2tp
21  21 LAC  ESTABLISHED joe50@l2tp
22  22 LAC  ESTABLISHED joe51@l2tp
```

The following example shows output for the **show l2tp info** command when a specific peer, tunnel, and session are named:

```
[local]RedBack>show l2tp info peer lac tunnel 1 session 2

Tx Data Packets: 4                    Rx Data Packets: 3
Tx Data Bytes: 118                    Rx Data Bytes: 66
```

Related Commands

ethernet encapsulation
l2tp-peer name
show l2tp counters

static

static

no static

Purpose

Maintains at least one tunnel to the Layer 2 Tunneling Protocol (L2TP) peer at all times.

Command Mode

L2TP configuration

Syntax Description

This command has no keywords or arguments.

Default

Tunnels are established on demand.

Usage Guidelines

Use the **static** command to ensure that at least one tunnel to the peer is always maintained. When maintaining one tunnel to the peer at all times, the tunnel is always up, even if no sessions are active. If the value set by the **max-tunnels** command is greater than 1, a minimum of one tunnel is maintained. This command takes effect immediately when executed.

You cannot use this command if you entered L2TP configuration mode using either the **l2tp-peer unnamed** command or the **l2tp-peer default** command.

Use the **no** form of this command to configure the peer in such a way that tunnels are established on demand.

Examples

The following example configures the peer so that at least one tunnel is maintained, whether or not there are any active sessions:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#static
```

Related Commands

l2tp-peer name
max-tunnels

timeout

timeout *seconds*

default timeout

Purpose

Sets the amount of time to wait for an acknowledgment before a control message is retransmitted to a Layer 2 Tunneling Protocol (L2TP) peer.

Command Mode

L2TP configuration

Syntax Description

seconds	Number of seconds to wait for an acknowledgment. The range of values is 1 to 255; the default value is 6.

Default

The timeout period is set to six seconds.

Usage Guidelines

Use the **timeout** command to set the amount of time to wait for an acknowledgment before a control message is retransmitted to a peer. You should only increase the value if many sessions are established or if the media is slow.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to reset the timeout to six seconds.

Examples

The following example configures the peer so that retransmission of a control message occurs after 5 seconds without an acknowledgment:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#timeout 5
```

Related Commands

clear tunnel
retry
tunnel-window

tunnel-auth

tunnel-auth *secret*

no tunnel-auth

Purpose

Sets the primary Layer 2 Tunneling Protocol (L2TP) password to the tunnel peer and enables tunnel authentication.

Command Mode

L2TP configuration

Syntax Description

secret	Primary L2TP password for the tunnel. The password can be any alphanumeric text string of any length.

Default

No password is created.

Usage Guidelines

Use the **tunnel-auth** command to set the primary L2TP password to the tunnel peer and enable tunnel authentication. If you do not use the **tunnel-auth** command, no tunnel authentication is initiated by the tunnel endpoint, and no response is generated to a tunnel authentication challenge from the peer. You can establish a secondary password using the **secondary-tunnel-auth** command.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to delete any previously established primary password.

Examples

The following example establishes `6dkq7pv` as the primary L2TP peer password:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#tunnel-auth 6dkq7pv
```

Related Commands

clear tunnel
l2tp-peer name
secondary-tunnel-auth

tunnel domain

tunnel domain

no tunnel domain

Purpose

Dynamically maps a subscriber's Point-to-Point Protocol (PPP) session to a Layer 2 Tunneling Protocol (L2TP) tunnel peer that has the same name as the user's domain name.

Command Mode

subscriber configuration

Syntax Description

This command has no keywords or arguments.

Default

A PPP session is terminated and routed rather than tunneled.

Usage Guidelines

Use the **tunnel domain** command to dynamically map a subscriber's PPP session to an L2TP tunnel peer that has the same name as the user's domain name. The tunnel must have the same name as the user's domain name (the *@context* portion of the default structured username format, for example). Create alias names for the context using the **domain** command in context configuration mode.

Note In general, we recommend that you use this command for the default subscriber, rather than an individual subscriber record.

The **tunnel name** command, which statically maps a specified tunnel peer, and the **tunnel domain** command are mutually exclusive.

Use the **no** form of this command to disable dynamic mapping in the subscriber record.

Examples

The following example configures the default subscriber record PPP sessions to be mapped to the tunnel that has the same name as the user's domain name:

```
[local]lac.telco.com(config)#context local
[local]lac.telco.com(config-ctx)#subscriber default
[local]lac.telco.com(config-sub)#tunnel domain
```

Related Commands

context
domain
tunnel domain
subscriber

tunnel name

tunnel name *tun-name*

no tunnel name *tun-name*

Purpose

Statically maps the subscriber's Point-to-Point Protocol (PPP) session to a specified Layer 2 Tunneling Protocol (L2TP) tunnel peer or L2TP group.

Command Mode

subscriber configuration

Syntax Description

tun-name	Name of the tunnel peer or L2TP group to be mapped.

Default

A PPP session is terminated rather than tunneled.

Usage Guidelines

Use the **tunnel name** command to force the subscriber to use a specific tunnel peer. A user cannot dynamically select a tunnel. The *group-name* argument value specified in the **l2tp-group name** command in context configuration mode can be used as the *tun-name* argument.

The **tunnel name** and **tunnel domain** commands are mutually exclusive.

Use the **no** form of this command to remove a statically mapped tunnel from a subscriber record.

Examples

The following example forces the subscriber to use the specified tunnel:

```
[local]lac.telco.com(config)#context local
[local]lac.telco.com(config-ctx)#subscriber name fred
[local]lac.telco.com(config-sub)#tunnel name freds-corp.com
```

Related Commands

l2tp attribute calling-number real-circuit-id
tunnel domain

tunnel-window

tunnel-window *messages*

default tunnel-window

Purpose

Sets the number of control messages a tunnel peer can send without acknowledgment from the Subscriber Management System (SMS) device.

Command Mode

L2TP configuration

Syntax Description

messages	Number of messages the peer can send without acknowledgment from the SMS device. The range of values is 1 to 65,535; the default value is 10.

Default

Up to 10 control messages can be sent by a peer without acknowledgment from the SMS device.

Usage Guidelines

Use the **tunnel-window** command to set the number of control messages a peer can send without acknowledgment from the SMS device. You might need to change the default number of messages, depending on the number of control messages a peer can generate at one time. For example, if a peer is bringing up many sessions at once, you might need to increase the number of messages.

Changing the configuration of a peer (or peer group) with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to set the number of control messages that can be sent without acknowledgment to 10.

Examples

The following example configures the peer to be able to send up to 15 control messages without acknowledgment from the SMS device:

```
[local]RedBack(config-ctx)#l2tp-peer name peer1
[local]RedBack(config-l2tp)#tunnel-window 15
```

Related Commands

clear tunnel
retry

L2F Commands

This chapter describes all commands related to configuring Layer 2 Forwarding (L2F) protocol tunnel peers. L2F peers are configured in L2F configuration mode. Use the **l2f-peer name** context configuration mode command to enter L2F configuration mode.

Note Unless otherwise indicated in the documentation for individual commands, changing the configuration of a peer with an established tunnel takes effect only upon issuing a **clear tunnel** command.

For overview information, a description of the tasks used to configure L2F peers, and configuration examples, see the "Configuring L2F" chapter in the *Access Operating System (AOS) Configuration Guide*.

clear tunnel

clear tunnel {**group** *group-name* | **peer** *peer-name* [**tunnel** *tunnel-id* [**session** *session-id*]]}

Purpose

Shuts down all or specified tunnels or sessions to a Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F) peer, or to the members of an L2TP group.

Command Mode

administrator exec

Syntax Description

group *group-name*	Name of an L2TP group.
peer *peer-name*	Name of an L2TP or L2F peer.
tunnel *tunnel-id*	Optional when you use the **peer** *peer-name* construct. Tunnel number of a particular L2TP or L2F tunnel to be shut down.
session *session-id*	Optional when you use the **tunnel** *tunnel-id* construct. Session number of a particular L2TP or L2F session to be shut down.

Default

No tunnels are cleared.

Usage Guidelines

Use the **clear tunnel** command to clear L2TP or L2F tunnels or sessions. For L2TP and L2F peers, you can shut down all tunnels to a specified peer if you use the **clear tunnel** command without any optional parameters. To shut down a specific tunnel and all the sessions within that tunnel, specify it by using the **tunnel** *tunnel-id* construct. To shut down a specific session, specify the tunnel and session by using both optional constructs.

For L2TP groups, this command allows you to clear all sessions and tunnels connected to the members of the group. Although all sessions and tunnels are cleared from members of the group, the group itself remains intact.

For Remote Authentication Dial-In User Service (RADIUS)-based configuration, this command is useful when you want a new configuration to be used. After this command is executed, the next RADIUS connection reads the new configuration.

Examples

The following command clears all tunnels to an L2F peer named one.net:

```
[local]RedBack#clear tunnel peer one.net
```

Related Commands

show l2f counters
show l2f info

debug l2x

debug l2x {**aaa** | **all** | **filter** | **packets** | **ses-setup** | **ses-state** | **tun-setup** | **tun-state** | **window**}

no debug l2x {**aaa** | **all** | **filter** | **packets** | **ses-setup** | **ses-state** | **tun-setup** | **tun-state** | **window**}

Purpose

Enables the logging of Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F) debugging messages.

Command Mode

administrator exec

Syntax Description

aaa	Enables L2TP and L2F authentication, authorization, and accounting (AAA) debugging.
all	Enables all L2TP and L2F debugging.
filter	Configures an L2TP and L2F debugging filter.
packets	Enables L2TP and L2F packet-level debugging.
ses-setup	Enables L2TP and L2F session-setup debugging.
ses-state	Enables L2TP and L2F session state-change debugging.
tun-setup	Enables L2TP and L2F tunnel-setup debugging.
tun-state	Enables L2TP and L2F tunnel state-change debugging.
window	Enables L2TP and L2F control-window debugging.

Default

L2TP and L2F debugging are disabled.

Usage Guidelines

Use the **debug l2x** command to enable the logging of L2TP and L2F debug messages. Use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable L2TP and L2F debugging.

Examples

The following command enables all types of debug logging for L2TP and L2F:

```
[local]RedBack#debug l2x all
```

Related Commands

l2f-peer name
logging console
show debugging
terminal monitor
tunnel domain
tunnel name

description

description *text*

no description

Purpose

Creates a textual description of a Layer 2 Forwarding (L2F) peer.

Command Mode

L2F configuration

Syntax Description

text	Textual description of an L2F peer. Can be any alphanumeric string, including spaces, that is not longer than one line. The text does not wrap to the next line.

Default

No description is associated with the peer.

Usage Guidelines

Use the **description** command to associate descriptive information with the name of the L2F peer. The textual description appears in the output of the **show configuration** command. To change a description, create a new one and it overwrites the existing one.

Use the **no** form of this command to delete an existing textual description.

Examples

The following example specifies (or creates) an L2F peer and then associates a text description with it:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#description NAS in California
```

The following example changes the existing description:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#description NAS in Southern California
```

The following example removes the existing description:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#no description
```

Related Commands

show configuration

domain

domain *dom-name*

no domain *dom-name*

Purpose

Creates an alias for the Layer 2 Forwarding (L2F) tunnel that can be used anywhere that the *peer-name* argument in the **l2f-peer name** command can be used.

Command Mode

L2F configuration

Syntax Description

dom-name	Name to be used as an alias. Cannot be a name that is already being used as a peer name or a domain name.

Default

No aliases are created.

Usage Guidelines

Use the **domain** command to create simpler names (for example, isp.net) than the *peer-name* argument, which is often a fully qualified domain name (for example, hssi_0_5.chi_core.isp.net). You can use multiple **domain** commands per-L2F peer in the configuration.

An L2F peer domain name cannot be the same as an existing L2F peer or domain name. Maintain unique names for all peers and domains. Also, within a single context, L2F and Layer 2 Tunneling Protocol (L2TP) peer and domain names must be unique from one another.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to remove the specified domain name as an alias.

Examples

The following example selects (or creates) an L2F peer and creates a domain name (alias) for it:

```
[local]RedBack(config-ctx)#l2f-peer name tanpeer1_1_5.xxx.core.isp.net
[local]RedBack(config-l2f)#domain corporate
```

Related Commands

show l2f counters
show l2f info

function

function {**nas** | **home-gateway**}

default function

Purpose

Specifies that only Network Access Server (NAS) or home gateway functionality is to be enabled for a Layer 2 Forwarding (L2F) peer.

Command Mode

L2F configuration

Syntax Description

nas	Specifies that only NAS functionality is enabled for an L2F peer.
home-gateway	Specifies that only home gateway functionality is enabled for an L2F peer.

Default

The peer performs the NAS function.

Usage Guidelines

Use the **function** command to specify either NAS or home gateway functionality on a peer. An L2F peer configuration may serve only as NAS or home gateway, but not both. If the peer is configured with NAS functionality, it sends, but does not accept, initial confirmation (CONF) messages. If the peer is configured with home gateway functionality, it accepts, but does not send, initial CONF messages.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of the command to specify that the peer perform the NAS function.

Examples

The following example specifies that the named L2F peer configuration will function as a NAS:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#function nas
```

Related Commands

l2f-peer name
show l2f info

l2f-peer name

l2f-peer name *peer-name* **media** {**udp-ip remote** {**ip** *ipaddr* | **dns** *dns-name*} [**local** *ipaddr*]}

no l2f-peer name *peer-name*

Purpose

Creates or selects a Layer 2 Forwarding (L2F) peer and enters L2F configuration mode.

Command Mode

context configuration

Syntax Description

peer-name	Name of the L2F tunnel peer. L2F peer names must be unique from other peer names or peer domain names. Within a context, L2F peer names must also be unique from Layer 2 Tunneling Protocol (L2TP) peer and domain names.
media udp-ip	Specifies a UDP/IP-encapsulated tunnel. At this time, only User Datagram Protocol (UDP)/IP encapsulation is available.
remote ip *ipaddr*	Remote IP address. Required for **udp-ip** encapsulation.
remote dns *dns-name*	Remote Domain Name System (DNS) name.
local *ipaddr*	Optional. Local IP address.

Default

None

Usage Guidelines

Use the **l2f-peer name** command to define an L2F peer and enter L2F configuration mode. The name of the L2F tunnel peer must be the same as the name that is provided by the peer as a hostname in Start-Control-Connection-Request (SCCRQ) packets. You can create an alias name for the tunnel with the **domain** command in L2F configuration mode.

L2F peer names and peer domain names must be unique. For example, if a peer is named john, no other L2F peer or peer domain can be named john. Also, within a single context, an L2F peer (or domain) cannot have the same name as an L2TP peer (or domain).

Use the **no** form of this command to delete an existing L2F tunnel peer.

Examples

The following example creates an L2F tunnel peer named `cr1.net`:

```
[local]RedBack(config-ctx)#l2f-peer name cr1.net media udp-ip remote ip 155.53.200.150
local 10.11.0.254
[local]Redback(config-l2f)#
```

Related Commands

show l2f info

l2x profile

l2x profile *prof-name*

no l2x profile *prof-name*

Purpose

Creates a Layer 2 Tunneling Protocol or Layer 2 Forwarding (L2X) tunnel profile and enters L2X profile configuration mode.

Command Mode

context configuration

Syntax Description

prof-name	Name of the tunnel profile to be created or modified.

Default

No L2X profile is created.

Usage Guidelines

Use the **l2x profile** command to create a new L2X profile that can subsequently be applied to a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) peer. This command also enters L2X profile configuration mode. Once in L2X profile configuration mode, you can use the **min-subscribers** command to set the minimum number of subscriber slots that are to be reserved for all the peers (combined) to which the profile is assigned.

Use the **no** form of this command to delete the profile from the configuration.

Examples

The following example creates an L2X profile called `winessential` and enters L2X profile configuration mode:

```
[local]RedBack(config-ctx)#l2x profile winessential
[local]RedBack(config-l2xprof)#
```

The following example applies the L2X profile called `winessential` to an L2F peer called `absolute`:

```
[local]RedBack(config-ctx)#l2tp-peer name absolute media pvc
[local]RedBack(config-l2tp)#profile winessential
```

See the **profile** command description in this chapter for more information on applying a profile to a peer.

Related Commands

min-subscribers
profile
show subscribers

local-name

local-name *hostname*

no local-name

Purpose

Sets the local hostname for an outbound confirmation (CONF) message.

Command Mode

L2F configuration

Syntax Description

hostname	Local hostname.

Default

The system hostname as specified by the **system hostname** global configuration command is used as the local hostname.

Usage Guidelines

Use the **local-name** command when more than one tunnel, with different characteristics, are required for the same peer.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to delete the specification of local hostname. To change a local hostname, create a new one and it overwrites the existing one.

Examples

The following example specifies the local hostname as `major`:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#local-name major
```

Related Commands

clear tunnel
system hostname

max-sessions

max-sessions *maxses*

no max-sessions

Purpose

Sets the maximum number of sessions allowed per tunnel for this Layer 2 Forwarding (L2F) peer configuration.

Command Mode

L2F configuration

Syntax Description

maxses	Maximum number of sessions allowed per tunnel. The range of values is 1 to 65,355; the default value is 65,355.

Default

The maximum number of sessions allowed per tunnel is the maximum number in the valid range (65,355).

Usage Guidelines

Use the **max-sessions** command to set the maximum number of sessions allowed per tunnel on the peer. For User Datagram Protocol (UDP) tunnels, a new tunnel opens if the *maxses* argument value has been reached for the current tunnel and the maximum number of tunnels (*maxtun* argument value in the **max-tunnels** command) has not been exceeded.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to set the maximum number of sessions per tunnel to 65,355.

Examples

The following example sets the maximum number of sessions allowed per tunnel to `1000`:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#max-sessions 1000
```

Related Commands

clear tunnel
max-tunnels

max-tunnels

max-tunnels *maxtun*

no max-tunnels

Purpose

Sets the maximum number of tunnels allowed for the a Layer 2 Forwarding (L2F) peer.

Command Mode

L2F configuration

Syntax Description

maxtun	Maximum number of tunnels allowed. The range of values is 1 to 128; the default value is 1.

Default

One tunnel is allowed per peer.

Usage Guidelines

Use the **max-tunnels** command to set the maximum number of tunnels allowed for the peer. Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to set the maximum number of tunnels allowed to 1.

Examples

The following example sets the maximum number of tunnels allowed to 2:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#max-tunnels 2
```

Related Commands

clear tunnel
max-sessions

min-subscribers

min-subscribers *sub-num*

no min-subscribers

Purpose

Establishes a minimum number of subscriber slots to be reserved for the combined tunnel peers to which the Layer 2 Tunneling Protocol or Layer 2 Forwarding (L2X) profile is applied.

Command Mode

L2X profile configuration

Syntax Description

sub-num	Number of subscriber slots to be reserved.

Default

No subscriber slots are reserved.

Usage Guidelines

Use the **min-subscribers** command to set the minimum number of subscriber slots to be reserved for the peers to which the L2X profile is applied. All the peers to which the profile is applied share the minimum number of reserved subscriber slots specified by the **min-subscribers** command. If, for example, the profile specifies that a minimum of 1,200 subscriber slots are to be reserved, and the profile is applied to four peers, then the 1,200 subscribers slots are reserved for all four of those peers combined.

Use the **no** form of this command to remove the reserved minimum from the configuration of the profile.

Examples

The following example configures the profile named `apples` to have a minimum of `1500` reserved subscriber slots:

```
[local]RedBack(config-ctx)#l2x profile apples
[local]RedBack(config-l2xprof)#min-subscribers 1500
```

Related Commands

l2x profile
show subscribers

police

police rate *rate* **burst** *size*

no police

Purpose

Limits the aggregate packet stream received over a Layer 2 Forwarding (L2F) tunnel by rate and burst tolerance.

Command Mode

L2F configuration

Syntax Description

rate *rate*	Limiting rate in kbps. The range of values is 10 to 155,520 kbps.
burst *size*	Burst tolerance size in bytes. The range of values is 0 to 100,000 bytes.

Default

No limiting rate or burst tolerance is set.

Usage Guidelines

Use the **police** command to control incoming traffic. A general rule to determine burst tolerance is to multiply the link MTU by 10 (around 15,000 to 20,000 bytes for subscriber circuits). A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and burst tolerance are dropped.

If the value set by the **max-tunnels** command is greater than 1, the **police** command sets the rate for each tunnel. Only tunnels established after the **police** command has been entered are affected.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to remove any previously set limiting rate or burst size limitations.

Examples

The following example sets limitations on the rate and burst size of incoming traffic through the tunnel:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#police rate 12 burst 17000
```

Related Commands

clear tunnel
max-tunnels
rate-limit

profile

profile *prof-name*

no profile *prof-name*

Purpose

Applies a Layer 2 Tunneling Protocol or Layer 2 Forwarding (L2X) profile to a Layer 2 Forwarding (L2F) peer.

Command Mode

L2F configuration

Syntax Description

prof-name	Name of the tunnel profile to be applied to the peer.

Default

None

Usage Guidelines

Use the **profile** command to apply a tunnel profile to an L2F peer. All the peers to which the profile is applied share the minimum number of reserved subscriber slots specified in the configuration of the profile. If, for example, the profile specifies that a minimum of 1,200 subscriber slots are to be reserved, and the profile is applied to four peers, then the 1,200 subscriber slots are reserved for all four of those peers combined.

You can apply a profile to Layer 2 Tunneling Protocol (L2TP) and L2F peers, and you can configure multiple profiles in a context. The total number of reserved subscriber slots designated in a context's profiles cannot exceed the number reserved for the context as a whole using the **aaa min-subscribers** command. However, it is not necessary to have the **aaa min-subscribers** command in the configuration to reserve subscriber slots for tunnel peers using the **profile** command.

Use the **no** form of this command to disassociate the peer from the profile.

Examples

The following example applies the L2X profile called `winessential` to an L2F peer called `absolute`:

```
[local]RedBack(config-ctx)#l2tp-peer name absolute media pvc
[local]RedBack(config-l2tp)#profile winessential
```

Related Commands

aaa min-subscribers
l2x profile
min-subscribers
show subscribers

rate-limit

rate-limit rate *rate* **burst** *size*

no rate-limit

Purpose

Limits the aggregate packet stream transmitted over a Layer 2 Forwarding (L2F) tunnel by rate and burst tolerance.

Command Mode

L2F configuration

Syntax Description

rate *rate*	Limiting rate in kbps. The range of values is 10 through 155,520 kbps.
burst *size*	Burst tolerance size in bytes. The range of values is 0 through 100,000 bytes.

Default

There is no limitation on the rate and burst size of outgoing traffic.

Usage Guidelines

Use the **rate-limit** command to control outgoing traffic. A general rule to determine burst tolerance is to multiply the link MTU by 10 (around 15,000 to 20,000 bytes for subscriber circuits). A larger burst tolerance is generally appropriate for backhaul circuits. Packets exceeding the specified rate and burst tolerance are dropped.

If the value set by the **max-tunnels** command is greater than 1, the **rate-limit** command sets the rate for each tunnel. Only tunnels established after the **rate-limit** command has been entered are affected.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to remove any previously set limitation.

Examples

The following example sets limitations on the rate limit and burst size of outgoing traffic through the tunnel:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#rate-limit rate 12 burst 17000
```

Related Commands

clear tunnel
max-tunnels
police

retry

retry *count*

default retry

Purpose

Sets the number of times an unacknowledged control message is retransmitted to a Layer 2 Forwarding (L2F) peer before the tunnel is brought down.

Command Mode

L2F configuration

Syntax Description

count	Number of times an unacknowledged control message is retransmitted to a peer. The range of values is 1 through 255; the default value is 5.

Default

An unacknowledged control message is retransmitted five times.

Usage Guidelines

Use the **retry** command to set the number of times an unacknowledged control message is retransmitted to a peer before the tunnel is brought down. You may want to increase the value from the default of 5 if the L2F media is not reliable.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to set the number of retransmissions to 5.

Examples

The following example configures the peer so that unacknowledged control messages are retransmitted six times before the tunnel is brought down:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#retry 6
```

Related Commands

clear tunnel
timeout

session-auth

session-auth {**pap** | **chap** | **chap pap**} [**context** *ctx-name* | **service-group** *group-name*]

default session-auth

Purpose

Specifies the method used by a home gateway to authenticate subscriber sessions that arrive over this Layer 2 Forwarding (L2F) tunnel.

Command Mode

L2F configuration

Syntax Description

pap	Specifies that Password Authentication Protocol (PAP) is to be used to obtain the username and password from the subscriber.
chap	Specifies that Challenge Handshake Authentication Protocol (CHAP) is to be used to obtain the username and password from the subscriber.
chap *pap*	Specifies that either PAP or CHAP can be used to obtain the username and password from the subscriber, but that CHAP is preferred.
context *ctx-name*	Optional. Name of a specific context to which subscriber sessions are restricted.
service-group *group-name*	Optional. Name of a service access list that limits the services available to the circuit or port.

Default

CHAP or PAP can be used as an authentication method.

Usage Guidelines

Use the **session-auth** command to specify the method used by an L2F home gateway to authenticate subscriber sessions that arrive over the tunnel. Use the optional **context** *ctx-name* construct to prevent dynamic context selection, thereby limiting the services available to any PPP sessions that arrive from this peer. Specifically, these sessions are limited to terminating and routing in the named context and to entering a tunnel defined within that context. If the **context** *ctx-name* construct is present, the Access Operating System (AOS) attempts to authenticate the session according to the authentication, authorization, and accounting (AAA) configuration for the named context, rather than according to the context portion of the structured username, if present. If the user passes authentication, the session comes up.

If Remote Authentication Dial-In User Service (RADIUS) returns a Context-Name attribute whose value conflicts with the **context** *ctx-name* construct (or any of its aliases) in the command line, the binding fails. Authentication also fails if global authentication is configured and the Access-Response packet from the RADIUS server does not contain a Context-Name attribute.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to set the home gateway to use CHAP PAP to authenticate subscriber sessions.

Examples

The following example establishes that either PAP or CHAP can be used to authenticate subscriber sessions:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#session-auth chap pap
```

Related Commands

clear tunnel
function

show l2f counters

show l2f counters [**peer** *peer-name* [**tunnel** *tunnel-id* [**session** *session-id*]]]

Purpose

Displays the statistics for Layer 2 Forwarding (L2F) tunnel peers.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Optional. Specific peer about which you want information displayed.
tunnel *tunnel-id*	Optional when you use the **peer** *peer-name* construct. Tunnel number of the tunnel for which you want information displayed.
session *session-id*	Optional when you use the **tunnel** *tunnel-id* construct. Session number of the session for which you want information displayed.

Default

Displays counters for all L2F peers in the current context.

Usage Guidelines

Use the **show l2f counters** command to see the following L2F tunnel statistics:

- Peer name
- Number of transmitted (tx) packets (outgoing)
- Number of received (rx) packets (incoming)
- Number of tunnels bound to this peer in any state (up, coming up, or down)
- Total number of control message errors (each tunnel has one control channel)
- Total number of sessions to the peer in any state (up, coming up, or down)
- Number of sessions disconnected by a peer
- Number of tunnel failures (retries exceeded)

Examples

The following example shows the output for a Network Access Server (NAS) with a peer named `badger` and tunnel ID of `1`. You can see that each of the first five sessions are bound with the **bind session** command.

```
[local]RedBack>show l2f counters peer badger tunnel 1

Tx Data Packets:            93          Rx Data Packets:           110
Tx Data Bytes:            2409          Rx Data Bytes:            3264
Tx Control Packets:         54          Rx Control Packets:         54
Tx Control Bytes:         3808          Rx Control Bytes:         1222
Police pkts drops:           0          Rate pkts drops:             0

Tunnel Ctl Errors:      0
Last Ctl Error:     (NONE)
Last Ctl Err Time:  (NO TIME)

Tunnel Data Errors:     0
Last Data Error:        0
Last Data Err Time: (NO TIME)

Tx SCCRQ Count:         1
Tx Last SCCRQ Time: FRI MAY 19 08:32:04 2023
Tx Last SCCCN Time: FRI MAY 19 08:32:04 2023

Rx SCCRQ Count:         0
Rx Last SCCRQ Time: (NO TIME)
Rx Last SCCCN Time: (NO TIME)

Active Sessions:       10

 Ses   Rem
 ID    ID   Type  Tx Pkts    Rx Pkts   State       PPP Subscriber
----- ----- ---- ---------- ---------- ----------- --------------------
    2     2 NAS           6          7 ESTABLISHED (NO SUBSCRIBER)
    3     3 NAS           6          7 ESTABLISHED (NO SUBSCRIBER)
    4     4 NAS           6          7 ESTABLISHED (NO SUBSCRIBER)
    5     5 NAS           6          7 ESTABLISHED (NO SUBSCRIBER)
    6     6 NAS           6          7 ESTABLISHED (NO SUBSCRIBER)
   13    18 NAS           4          4 ESTABLISHED joe32@l2f
   14    19 NAS           4          4 ESTABLISHED joe33@l2f
   15    20 NAS           4          4 ESTABLISHED joe34@l2f
   16    21 NAS           3          4 ESTABLISHED joe35@l2f
   17    22 NAS           3          4 ESTABLISHED joe36@l2f
```

The following example shows the output for a home gateway peer named `racoon` with a tunnel ID of `1`:

```
[local]RedBack>show l2f counters peer racoon tunnel 1

Tx Data Packets:           308          Rx Data Packets:           247
Tx Data Bytes:            8935          Rx Data Bytes:            5733
```

```
Tx Control Packets:        211          Rx Control Packets:        210
Tx Control Bytes:         4379          Rx Control Bytes:        17937
Police pkts drops:           0          Rate pkts drops:             0

Tunnel Ctl Errors:           0
Last Ctl Error:          (NONE)
Last Ctl Err Time:   (NO TIME)

Tunnel Data Errors:          0
Last Data Error:             0
Last Data Err Time:  (NO TIME)

Tx SCCRQ Count:              0
Tx Last SCCRQ Time: (NO TIME)
Tx Last SCCCN Time: (NO TIME)

Rx SCCRQ Count:              1
Rx Last SCCRQ Time: MON SEP 03 14:19:12 2040
Rx Last SCCCN Time: MON SEP 03 14:19:12 2040

Active Sessions:       12

 Ses   Rem
 ID    ID   Type  Tx Pkts    Rx Pkts   State       PPP Subscriber
----- ----- ---- ---------- ---------- ----------- --------------------
 2     2    HG    4          4         ESTABLISHED joe37@l2f
 3     3    HG    4          4         ESTABLISHED joe38@l2f
 4     4    HG    4          4         ESTABLISHED joe39@l2f
 5     5    HG    4          3         ESTABLISHED joe32@l2f
 6     6    HG    4          3         ESTABLISHED joe33@l2f
 7     7    HG    4          4         ESTABLISHED joe34@l2f
 8     8    HG    4          3         ESTABLISHED joe42@l2f
 9     9    HG    4          3         ESTABLISHED joe43@l2f
 10    10   HG    4          3         ESTABLISHED joe44@l2f
 11    11   HG    4          3         ESTABLISHED joe47@l2f
 12    12   HG    4          3         ESTABLISHED joe48@l2f
 13    13   HG    4          3         ESTABLISHED joe49@l2f
```

Related Commands

l2f-peer name
show l2f info

show l2f info

show l2f info [**peer** *peer-name* [**tunnel** *tunnel-id* [**session** *session-id*]]]

Purpose

Displays a summary of status and configuration for Layer 2 Forwarding (L2F) tunnels.

Command Mode

operator exec

Syntax Description

peer *peer-name*	Optional. Specific peer about which you want information displayed.
tunnel *tunnel-id*	Optional if you use the **peer** *peer-name* construct. Tunnel number of the tunnel for which you want to display information.
session *session-id*	Optional if you use the **tunnel** *tunnel-id* construct. Session number of the session for which you want to display information.

Default

Displays information about all L2F peers in the current context.

Usage Guidelines

Use the **show l2f info** command to see the following L2F tunnel status and configuration information:

- Peer name.
- Local name.
- Media type.
- Maximum number of tunnels for the specified peer.
- Total number of tunnels to the specified peer in any state (for example, up, coming up, or down).
- Maximum number of sessions for the specified peer.
- Total number of sessions for the specified peer in any state (for example, up, coming up, or down).
- Static command status (enabled or disabled).
- Whether this end of the tunnel is Network Access Server (NAS) enabled (**function nas** command).

- Whether this end of the tunnel is home gateway enabled (**function home-gateway** command).
- Whether the peer is named or unnamed. The tunnel includes a peer name in the first column. Check the Named column in the output to determine whether the peer is named or unnamed.

Examples

The following examples show output for the **show l2f info** command first with no keywords and then for a specific peer:

```
[local]RedBack>show l2f info

                              Max  Tun  Max Ses
Peer Name  Local Name  Med    Tuns Cnt  Ses Cnt  Stat NAS  HG  Named
---------  ----------- ----   ---- ---  --- ---- ---  ---  --- ----
l2f_1      tgrpl       UDP    1    1    20   20   NO  YES  YES  YES
l2f_2      tgrp2       UDP    1    1    20   20   NO  YES  YES  YES
pvc_l2f    tgrp3       PVC    1    1   65535 20   NO  YES  YES  YES


[local]RedBack>show l2f info peer l2f_1

Peer name:          l2f_1          Media:               UDP
Hostname alias:     tgrp1          RADIUS:              YES
Remote IP address:  11.1.1.2       Static:              NO
Local IP address:   11.1.1.1       Unnamed:             NO
NAS:                YES            Maximum Tunnels:     1
HG:                 YES            Maximum Ses/Tunnel:  20
Ctl retran timeout: 4              Ctl retran count:    3
Session auth:       CHAP PAP       Control window:      10
DNIS:               NO             DNIS ONLY:           NO
Police rate:        0              Police burst:        0
Rate-limit rate:    0              Rate-limit burst:    0
Group:              l2f            Preference:          1
Tunnel password:    jiffy
Domains:            vpn_1

Tunnel Count:       1              Tunnel Ctl Errors:   41
Session Count:      20             Tunnel Data Errors:  0

             Rem   Ses   Cntl  Last
Tunnel Name  ID    Cnt   Errs  Err      Remote IP / PVC State
-----------  ----  ---   ----  -------- ---------- --------------
l2f:1        1     20    41    REXMT    11.1.1.2    ESTABLISHED
```

Related Commands

l2f-peer name
show l2f counters

timeout

timeout *seconds*

default timeout

Purpose

Sets the amount of time to wait for an acknowledgment before a control message is retransmitted to a Layer 2 Forwarding (L2F) peer.

Command Mode

L2F configuration

Syntax Description

seconds	Number of seconds to wait for an acknowledgment. The range of values is 1 through 255; the default value is 4.

Default

The timeout period is set to 4 seconds.

Usage Guidelines

Use the **timeout** command to set the amount of time to wait for an acknowledgment before a control message is retransmitted to a peer. You should only increase the value over the default if many sessions are established or if the media is slow.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **default** form of this command to reset the timeout to four seconds.

Examples

The following example configures the peer so that retransmission of a control message occurs after 5 seconds without an acknowledgment:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#timeout 5
```

Related Commands

clear tunnel
retry

tunnel-auth

tunnel-auth local *secret1* **remote** *secret2*

no tunnel-auth

Purpose

Sets the Layer 2 Forwarding (L2F) passwords to the tunnel peer and enables tunnel authentication.

Command Mode

L2F configuration

Syntax Description

local *secret1*	Local tunnel password sent by this Subscriber Management System (SMS) device to the L2F peer. The password can be any alphanumeric text string of any length.
remote *secret2*	Remote tunnel password that must match that sent by the remote peer. The password can be any alphanumeric text string of any length.

Default

None

Usage Guidelines

Use the **tunnel-auth** command to set the L2F password to the tunnel peer and enable tunnel authentication. If you do not use the **tunnel-auth** command, no tunnel authentication is initiated by the tunnel endpoint and no response is generated to a tunnel authentication challenge from the peer.

Changing the configuration of a peer with an established tunnel does not take effect until you delete all tunnels to the peer (using the **clear tunnel** command), or until all the tunnels to the peer come down naturally. The configuration database is queried again to reestablish tunnels to the peer, thereby implementing the new configuration.

Use the **no** form of this command to delete any previously established password.

Examples

The following example establishes `6dkq7pv` as the local L2F peer password and `zzz` as the remote password:

```
[local]RedBack(config-ctx)#l2f-peer name peer1
[local]RedBack(config-l2f)#tunnel-auth local 6dkq7pv remote zzz
```

Related Commands

clear tunnel
l2f-peer name

tunnel domain

tunnel domain

no tunnel domain

Purpose

Dynamically maps a subscriber's Point-to-Point Protocol (PPP) session to a Layer 2 Forwarding (L2F) tunnel peer that has the same name as the user's domain name.

Command Mode

subscriber configuration

Syntax Description

This command has no keywords or arguments.

Default

A PPP session is terminated and routed rather than tunneled.

Usage Guidelines

Use the **tunnel domain** command to dynamically map a subscriber's PPP session to an L2F tunnel peer that has the same name as the user's domain name.The tunnel must have the same name as the user's domain name (the *@context* portion of the default structured username format, for example). Create alias names for the context using the **domain** command in context configuration mode.

Note In general, we recommend that you use this command for the default subscriber, rather than an individual subscriber record.

The **tunnel name** command which statically maps a specified tunnel peer and the **tunnel domain** command are mutually exclusive.

Use the **no** form of this command to remove dynamic tunnel mapping from a subscriber record or from the default subscriber configuration‘.

Examples

The following example maps PPP sessions to the tunnel that has the same name as the user's domain name:

```
[local]lac.telco.com(config)#context local
[local]lac.telco.com(config-ctx)#subscriber default
[local]lac.telco.com(config-sub)#tunnel domain
```

Related Commands

context
domain
subscriber
tunnel name

tunnel name

tunnel name *tun-name*

no tunnel name *tun-name*

Purpose

Statically maps the subscriber's Point-to-Point Protocol (PPP) session to a specified Layer 2 Forwarding (L2F) tunnel peer.

Command Mode

subscriber configuration

Syntax Description

tun-name	Name of the tunnel peer to be mapped.

Default

A PPP session is terminated rather than tunneled.

Usage Guidelines

Use the **tunnel name** command to force the subscriber to use a specific tunnel peer. A user cannot dynamically select a tunnel.

The **tunnel name** and **tunnel domain** commands are mutually exclusive.

Use the **no** form of this command to remove a statically-mapped tunnel from a subscriber record.

Examples

The following example forces the subscriber to use the specified tunnel:

```
[local]lac.telco.com(config)#context local
[local]lac.telco.com(config-ctx)#subscriber name fred
[local]lac.telco.com(config-sub)#tunnel name freds-corp.com
```

Related Commands

tunnel domain

Part 7

Security

IPSec Commands

This chapter describes the commands used to configure IP Security (IPSec) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure IPSec features, and configuration examples, see the "Configuring IPSec" chapter in the *Access Operating System (AOS) Configuration Guide*.

ah hash

ah hash {**hmac-md5** | **hmac-md5-96** | **hmac-sha** | **hmac-sha-96** | **none**} [**key** *key-name*]

no ah hash

Purpose

Defines the hash algorithm to use for the authentication header (AH) in the proposal.

Command Mode

IPSec proposal configuration

Syntax Description

hmac-md5	Specifies that the hmac-md5 hash algorithm is to be used in the proposal.
hmac-md5-96	Specifies that the hmac-md5-96 hash algorithm is to be used in the proposal.
hmac-sha	Specifies that the hmac-sha hash algorithm is to be used in the proposal.
hmac-sha-96	Specifies that the hmac-sha-96 hash algorithm is to be used in the proposal.
none	Specifies that no hash algorithm is to be used in the proposal.
key *key-name*	Optional. Name of the key to be used in the case of manual tunnels.

Default

No hash algorithm is defined for the proposal.

Usage Guidelines

Use the **ah hash** command to specify the hash algorithm to use for AH. AH and the available hash algorithms are implemented in accordance with RFC 2402, *The Authentication Header.*

Hash algorithms are used to provide data integrity. The AH protocol for providing data integrity might be appropriate in cases where data integrity without encryption is desired.

Use the **key** *key-name* construct for manual tunnels only. Internet key exchange (IKE)-negotiated tunnels cannot have a key specification.

Use the **no** form of this command to remove the specification of hash algorithm from the proposal configuration.

Examples

The following example configures an AH hash algorithm for a manual proposal:

```
[local]RedBack(config-ipsec-proposal)#ah hash hmac-sha key wishcraft
```

Related Commands

esp cipher
esp hash

cipher

cipher {**des-cbc** | **3des-cbc** | **des-ecb** | **3des-ecb** | **none**}

no cipher

Purpose

Defines the cipher algorithm to use for this Internet key exchange (IKE) proposal.

Command Mode

IKE proposal configuration

Syntax Description

des-cbc	Specifies that the DES-CBC cipher algorithm is to be used in the proposal.
3des-cbc	Specifies that the 3DES-CBC cipher algorithm is to be used in the proposal.
des-ecb	Specifies that the DES-ECB cipher algorithm is to be used in the proposal.
3des-ecb	Specifies that the 3DES-ECB cipher algorithm is to be used in the proposal.
none	Specifies that no cipher algorithm is to be used in the proposal.

Default

No cipher algorithm is defined.

Usage Guidelines

Use the **cipher** command for IKE-negotiated tunnels only. Cipher algorithms provide encryption.

Use the **no** form of this command to remove the specification of cipher algorithm from the IKE proposal configuration.

Examples

The following example specifies a cipher algorithm for an IKE proposal:

```
[local]RedBack(config-ipsec-proposal_ike)#cipher des-cbc
```

Related Commands

hash
ipsec proposal ike name

clear ipsec peer

clear ipsec peer [**name** *peer-name* | **id** *tunnel-id*] [**no-restart**]

Purpose

Forces the specified IP Security (IPSec) tunnel to come down, and then brings it back up again using the latest configuration information as soon as an IP packet arrives that is destined for that tunnel.

Command Mode

administrator exec

Syntax Description

name *peer-name*	Optional. Name of the IPSec tunnel peer to be brought down.
id *tunnel-id*	Optional. Numeric ID (available in the output of the **show ipsec peer** command) of the IPSec tunnel about which you want status information.
no-restart	Optional. Specifies that once the peer is brought down, it is not to be automatically made available to be brought back up. If you use this keyword, the peer does not come back up until a subscriber requires it.

Default

If you do not use any of the optional constructs, the **clear ipsec peer** command brings down all IPSec peers, and then brings them all back up again as soon as an IP packet arrives that is destined for that tunnel.

Usage Guidelines

Use the **clear ipsec peer** command to bring down all IPSec peers, and then send the latest configuration information to the Transform Engine (TE) module, enabling it to bring each peer back up again as soon as an IP packet arrives that is destined for that tunnel.

Optionally, you can specify a peer name or tunnel ID to bring down only a specific peer.

If you use the optional **no-restart** keyword, the peers are not brought back up again. To bring up a peer that has been brought down and not restarted, a new subscriber must come up who requires the peer, or you must issue the **clear ipsec peer** command a second time, without the **no-restart** keyword.

Using the **clear ipsec peer** command to bring down a peer does not disconnect the subscribers that use the peer to pass traffic, although the ability of the subscriber's secure traffic to reach its destination is affected.

Examples

The following example clears the `corporate` IPSec peer, but does not make it available for restart:

```
[local]RedBack#clear ipsec peer name corporate no-restart
```

To bring the `corporate` peer back up prior to a subscriber requiring it, you can issue the command again as follows:

```
[local]RedBack#clear ipsec peer name corporate
```

Related Commands

show ipsec peer

debug ipsec ike

debug ipsec ike

no debug ipsec ike

Purpose

Enables IP Security (IPSec) Internet key exchange (IKE) negotiation debugging.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

IPSec IKE negotiation debugging is disabled.

Usage Guidelines

Use the **debug ipsec ike** command to enable IPSec IKE negotiation debugging. When IPSec IKE negotiation debugging is enabled, all IPSec IKE-related messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable IPSec IKE negotiation debugging.

Examples

The following command enables IPSec IKE negotiation debugging:

```
[local]Redback#debug ipsec ike
```

Related Commands

debug ipsec peer

debug ipsec peer

debug ipsec peer [*value*]

no debug ipsec peer

Purpose

Enables IP Security (IPSec) peer debugging.

Command Mode

administrator exec

Syntax Description

value	Optional. Integer from 1 to 7, indicating the level of debugging information to display. 1 displays the least detailed information and 7 displays the most detailed. If no *value* argument is specified, the default is 4.

Default

IPSec peer debugging is disabled.

Usage Guidelines

Use the **debug ipsec peer** command to enable IPSec peer debugging. When IPSec peer debugging is enabled, all IPSec peer-related messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable IPSec peer debugging.

Examples

The following example enables the most detailed level of IPSec peer debugging:

```
[local]Redback#debug ipsec peer 7
```

Related Commands

debug ipsec ike

encapsulation-mode

encapsulation-mode {**tunnel** | **transport**}

no encapsulation-mode

Purpose

Defines the encapsulation type for the IP Security (IPSec) proposal.

Command Mode

IPSec proposal configuration

Syntax Description

tunnel	Specifies the encapsulation mode as tunnel, used when forming IPSec tunnels directly between two Subscriber Management System (SMS) devices to carry encrypted traffic.
transport	Specifies the encapsulation mode as transport; used when it is necessary to encrypt Layer 2 Tunneling Protocol (L2TP) tunnels.

Default

The encapsulation mode for the IPSec proposal is set to tunnel.

Usage Guidelines

Use the **encapsulation-mode tunnel** command to specify that the proposal is to be used for either tunnel or transport mode. In tunnel mode, an IPSec tunnel is formed directly between two SMS devices to carry encrypted traffic for users. Use transport mode when, for example, the SMS device terminates asynchronous transport mode (ATM) permanent virtual circuits (PVC)s and then sends Point-to-Point Protocol (PPP) sessions to an upstream Internet service provider (ISP) using L2TP. Transport mode allows the SMS device to encrypt the L2TP tunnel so security is maintained from one end to the other.

Use the **no** form of this command to revert to the default encapsulation mode of tunnel.

Examples

The following example sets the encapsulation mode for the proposal to `transport`:

```
[local]RedBack(config-ctx)#ipsec proposal name fastrack
[local]RedBack(config-ipsec-proposal)#encapsulation-mode transport
```

Related Commands

ipsec proposal crypto name

esp cipher

esp cipher {**des-cbc** | **3des-cbc** | **des-ecb** | **3des-ecb** | **none**} [**key** *key-name*]

no esp cipher

Purpose

Defines the cipher algorithm to use for Encapsulating Security Payload (ESP) in this proposal.

Command Mode

IPSec proposal configuration

Syntax Description

des-cbc	Specifies that the des-cbc cipher algorithm is to be used in the proposal.
3des-cbc	Specifies that the 3des-cbc cipher algorithm is to be used in the proposal.
des-ecb	Specifies that the DES-ECB cipher algorithm is to be used in the proposal.
3des-ecb	Specifies that the 3DES-ECB cipher algorithm is to be used in the proposal.
none	Specifies that no cipher algorithm is to be used in the proposal.
key *key-name*	Optional. Name of the key to be used in the case of manual tunnels.

Default

No cipher algorithm is defined.

Usage Guidelines

Use the **esp cipher** command to define the cipher algorithm to use for ESP in the proposal. ESP and the available hash algorithms are implemented in accordance with RFC 2406, *IP Encapsulating Security Payload (ESP)*.

Cipher algorithms provide encryption. ESP has the ability to provide both data integrity and encryption. Use the **key** *key-name* construct for manual tunnels only. Internet key exchange (IKE)-negotiated tunnels cannot have a key specification.

Use the **no** form of this command to remove the specification of cipher algorithm from the proposal configuration.

Examples

The following example configures an ESP cipher algorithm for a manual proposal:

```
[local]RedBack(config-ipsec-proposal)#esp cipher des-cbc key absoxxu299
```

Related Commands

ah hash
esp hash
ipsec proposal crypto name

esp hash

esp hash {**hmac-md5** | **hmac-md5-96** | **hmac-sha** | **hmac-sha-96** | **none**} [**key** *key-name*]

no esp hash

Purpose

Defines the hash algorithm to use for Encapsulating Security Payload (ESP) in this proposal.

Command Mode

IPSec proposal configuration

Syntax Description

hmac-md5	Specifies that the hmac-md5 hash algorithm is to be used in the proposal.
hmac-md5-96	Specifies that the hmac-md5-96 hash algorithm is to be used in the proposal.
hmac-sha	Specifies that the hmac-sha hash algorithm is to be used in the proposal.
hmac-sha-96	Specifies that the hmac-sha-96 hash algorithm is to be used in the proposal.
none	Specifies that no hash algorithm is to be used in the proposal.
key *key-name*	Optional. Name of the key to be used in the case of manual tunnels.

Default

No hash algorithm is defined.

Usage Guidelines

Use the **esp hash** command to define the hash algorithm to be used for ESP in the proposal. ESP and the available hash algorithms are implemented in accordance with RFC 2406, *IP Encapsulating Security Payload (ESP)*.

Hash algorithms provide data integrity. ESP has the ability to provide both data integrity and encryption. Use the **key** *key-name* construct for manual tunnels only. Internet key exchange (IKE)-negotiated tunnels cannot have a key specification.

Use the **no** form of this command to remove the specification of hash algorithm from the proposal configuration.

Examples

The following example configures an ESP hash algorithm for a manual proposal:

```
[local]RedBack(config-ipsec-proposal)#esp hash hmac-md5 key awaxxu299
```

Related Commands

ah hash
esp cipher
ipsec proposal crypto name

hash

hash {**md5** | **sha** | **none**}

no hash

Purpose

Defines the hash algorithm to use for the Internet key exchange (IKE) proposal.

Command Mode

IKE proposal configuration

Syntax Description

md5	Specifies that the md5 hash algorithm is to be used in the IKE proposal.
sha	Specifies that the sha hash algorithm is to be used in the IKE proposal.
none	Specifies that no hash alorithm is to be used in the IKE proposal.

Default

No hash algorithm is defined.

Usage Guidelines

Use the **hash** command to specify a hash algorithm only for IKE-negotiated (as opposed to manual) tunnels. Hash algorithms are used to provide data integrity.

Use the **no** form of this command to remove the specification of hash algorithm from the IKE proposal configuration.

Examples

The following example specifies a hash algorithm for an IKE proposal:

```
[local]RedBack(config-ipsec-proposal_ike)#hash sha
```

Related Commands

cipher
ipsec proposal ike name

ike auth

ike auth pre-shared-keys

no ike auth

Purpose

Specifies the authentication method used when invoking Internet key exchange (IKE).

Command Mode

IPSec peer configuration

Syntax Description

pre-shared-keys	Specifies that the pre-shared keys method is to be used for authentication. Currently, this is the only type of authentication supported.

Default

The pre-shared keys method of authentication is used.

Usage Guidelines

Use the **ike auth** command to specify the authentication method to be used when invoking IKE. The pre-shared keys method of authentication (the only method supported at this time) is implemented according to RFC 2409, *The Internet Key Exchange (IKE)*.

Use the **no** form of this command to revert to the pre-shared keys method of authentication.

Examples

The following example configures pre-shared keys as the method of authentication to be used for invoking IKE:

```
[local]RedBack(config-ipsec-peer)#ike auth pre-shared-keys
```

Related Commands

ike pre-shared-key
ipsec peer name

ike group

ike group *group-num*

no ike group

Purpose

Specifies the Internet Security Association and Key Management Protocol (ISAKMP) group that is to be used by the Diffie-Hellman key exchange to construct key material for an Internet key exchange (IKE) Security Association (SA).

Command Mode

IPSec peer configuration

Syntax Description

group-num Valid ISAKMP group numbers are 1 through 5 as follows:

1 = 768-bit modular exponentiation group (MODP)
2 = 1024-bit MODP group
3 = Galois Field (GF)[2^{155}] group
4 = GF[2^{185}] group
5 = 1536-bit MODP group

Default

ISAKMP group number 1 is used.

Usage Guidelines

Use the **ike group** command only if you are using IKE negotiation. An **ike group** command in the configuration is ignored if you use manual negotiation.

Use the **no** form of this command to revert to group number 1.

Examples

The following example selects ISAKMP group `5` for purposes of constructing key material:

```
[local]RedBack(config-ipsec-peer)#ike group 5
```

Related Commands

ipsec peer name

ike lifetime hard kbytes

ike lifetime hard kbytes *kbytes*

no ike lifetime hard kbytes

Purpose

Specifies the number of kilobytes of data transferred through an Internet key exchange (IKE) Security Association (SA) before the SA is deleted.

Command Mode

IPSec peer configuration

Syntax Description

kbytes	Number of kilobytes of data transferred before the SA is deleted. The default value is 2,000.

Default

The hard limit is 2,000 kilobytes.

Usage Guidelines

Use the **ike lifetime hard kbytes** command to set the hard limit in terms of kilobytes of data. Use the **ike lifetime hard seconds** command to set the hard limit in terms of time. If you have both in your configuration, the initiating peer starts dropping traffic when either hard limit is reached.

When a hard limit is reached, the initiating peer continues renegotiating for a new SA. The tunnel stays intact, but traffic intended for the tunnel is dropped.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets hard limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ike lifetime hard kbytes 6000
[local]RedBack(config-ipsec-peer)#ike lifetime hard seconds 3000
```

Related Commands

ike lifetime hard seconds
ike lifetime soft kbytes
ike lifetime soft seconds
ipsec peer name

ike lifetime hard seconds

ike lifetime hard seconds *seconds*

no ike lifetime hard seconds

Purpose

Specifies the number of seconds from creation of the Internet key exchange (IKE) Security Association (SA) before the SA is deleted.

Command Mode

IPSec peer configuration

Syntax Description

seconds	Number of seconds from SA creation before the SA is deleted. The default value is 3,600.

Default

The hard limit is 3,600 seconds.

Usage Guidelines

Use the **ike lifetime hard seconds** command to set the hard limit in terms of time. Use the **ike lifetime hard kbytes** command to set the hard limit in terms of kilobytes of data. If you have both in your configuration, the initiating peer starts dropping traffic when either hard limit is reached.

When a hard limit is reached, the initiating peer continues renegotiating for a new SA. The tunnel stays intact, but traffic intended for the tunnel is dropped.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets hard limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ike lifetime hard kbytes 6000
[local]RedBack(config-ipsec-peer)#ike lifetime hard seconds 3000
```

Related Commands

ike lifetime hard kbytes
ike lifetime soft kbytes
ike lifetime soft seconds
ipsec peer name

ike lifetime soft kbytes

ike lifetime soft kbytes *kbytes*

no ike lifetime soft kbytes

Purpose

Specifies the number of kilobytes of data transferred through an Internet key exchange (IKE) Security Association (SA) before renegotiation for a new SA is started.

Command Mode

IPSec peer configuration

Syntax Description

kbytes	Number of kilobytes of data transferred before renegotiation is started. The default value is 1,800.

Default

The soft limit is 1,800 kilobytes.

Usage Guidelines

Use the **ike lifetime soft kbytes** command to set the soft limit in terms of kilobytes of data. Use the **ike lifetime soft seconds** command to set the soft limit in terms of time. If you have both in your configuration, the initiating peer begins the renegotiation when either soft limit is reached.

When a soft limit is reached, the initiating peer begins renegotiating for a new SA. The tunnel stays intact and secure traffic continues to be passed through the tunnel.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets soft limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ike lifetime soft kbytes 3000
[local]RedBack(config-ipsec-peer)#ike lifetime soft seconds 2200
```

Related Commands

ike lifetime hard kbytes
ike lifetime hard seconds
ike lifetime soft seconds
ipsec peer name

ike lifetime soft seconds

ike lifetime soft seconds *seconds*

no ike lifetime soft seconds

Purpose

Specifies the number of seconds from creation of the Internet key exchange (IKE) Security Association (SA) before renegotiation for a new SA is started.

Command Mode

IPSec peer configuration

Syntax Description

seconds	Number of seconds from SA creation before renegotiation begins. The default value is 3,240.

Default

The soft limit is 3,240 seconds.

Usage Guidelines

Use the **ike lifetime soft seconds** command to set the soft limit in terms of time. Use the **ike lifetime soft kbytes** command to set the soft limit in terms of kilobytes of data. If you have both in your configuration, the initiating peer begins renegotiation when either soft limit is reached.

When a soft limit is reached, the initiating peer begins renegotiating for a new SA. The tunnel stays intact and secure traffic continues to be passed through the tunnel.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets soft limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ike lifetime soft kilobytes 3000
[local]RedBack(config-ipsec-peer)#ike lifetime soft seconds 1800
```

Related Commands

ike lifetime hard kbytes
ike lifetime hard seconds
ike lifetime soft kbytes
ipsec peer name

ike pre-shared-key

ike pre-shared-key {**string** *string* | **hex** *binary*}

no ike pre-shared-key

Purpose

Defines the pre-shared key used in Internet key exchange (IKE) authentication.

Command Mode

IPSec peer configuration

Syntax Description

string *string*	Key to be used in IKE authentication. The **string** keyword is followed by an ASCII string.
hex *binary*	Key to be used in IKE authentication. The **hex** keyword is followed by a hexadecimal string.

Default

None

Usage Guidelines

Only use the **ike pre-shared-key** command when pre-shared keys is to be used as the method of authentication when invoking IKE. The pre-shared key can be specified as either an ASCII string or a hexadecimal string. You can only configure one pre-shared key for the peer.

Use the **no** form of this command to delete the key from the configuration.

Examples

The following example establishes an ASCII string pre-shared key:

```
[local]RedBack(config-ipsec-peer)#ike pre-shared-key string whereswanda
```

Related Commands

ike auth
ipsec peer name

ike sa_subnet

ike sa_subnet {*source source-wildcard* | **any**} {*destination destination-wildcard* | **any**}

no ike sa_subnet {*source source-wildcard* | **any**} {*destination destination-wildcard* | **any**}

Purpose

Configures the source and destination addresses for a local Internet key exchange (IKE) Security Association (SA) subnet.

Command Mode

IPSec peer configuration

Syntax Description

source	Source IP address of the SA subnet.
source-wildcard	Indication of which bits in the *source* argument are significant. Expressed as a 32-bit quantity in a 4-byte dotted-decimal formal. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source or destination IP address.
destination	Destination IP address of the SA subnet.
destination-wildcard	Indication of which bits in the *destination* argument are significant. Expressed as a 32-bit quantity in a 4-byte dotted-decimal formal. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.

Default

None

Usage Guidelines

Use the **ike sa_subnet** command to configure the source and destination addresses for a local Internet key exchange (IKE) Security Association (SA) subnet. Any packet whose source and destination IP addresses fall within this subnet are sent through the tunnel associated with the SA.

Use the **no** form of this command to delete configuration of the subnet.

Examples

The following example establishes an SA local subnet:

```
[local]RedBack(config-ipsec-peer)#ike sa_subnet 10.25.0.0 0.0.255.255 any
```

Related Commands

ike auth
ipsec peer name

in

in {**string** *string* | **hex** *binary*}

[**no**] **in**

Purpose

Defines the key used for the inbound Security Association (SA) of a manual tunnel.

Command Mode

IPSec key configuration

Syntax Description

string *string*	Key to be used for the inbound SA of a manual tunnel. The **string** keyword is followed by an ASCII string.
hex *binary*	Key to be used for the inbound SA of a manual tunnel. The **hex** keyword is followed by a hexadecimal string.

Default

No key is defined for the inbound SA.

Usage Guidelines

Use the **in** command only for tunnels using manual proposals. You can express the key either as an ASCII string or as a hexadecimal string.

Use the **no** form of this command to remove the key definition from the configuration.

Examples

The following example defines inbound and outbound keys:

```
[local]RedBack(config-ctx)#ipsec key name perfect
[local]RedBack(config-ipsec-key)#in string 494949jjf8fuueeeoo
[local]RedBack(config-ipsec-key)#out string 33jmdiid999fff
```

Related Commands

ipsec key name
out

ip-address local

ip-address local *local-ip-addr*

no ip-address local

Purpose

Defines the local IP address of the IP Security (IPSec) peer.

Command Mode

IPSec peer configuration

Syntax Description

local-ip-addr	Local IP address for the IPSec peer. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format.

Default

No local IP address is defined.

Usage Guidelines

Use the **ip-address local** command to configure the local IP address of the tunnel peer. The local address is considered to be the source, while the remote address is considered to be the destination.

Use the **no** form of this command to remove the local address configuration.

Examples

The following example configures the local and remote addresses for the `headquarters` IPSec tunnel peer:

```
[local]RedBack(config-context)#ipsec peer name headquarters
[local]RedBack(config-ipsec-peer)#ip-address local 10.1.1.2
[local]RedBack(config-ipsec-peer)#ip-address remote 20.2.1.1
```

Related Commands

ip-address remote
ipsec peer name

ip-address remote

ip-address remote *remote-ip-addr*

no ip-address remote

Purpose

Defines the remote IP address of the IP Security (IPSec) peer.

Command Mode

IPSec peer configuration

Syntax Description

remote-ip-addr	Remote IP address for the IPSec peer; expressed as a 32-bit quantity in a 4-byte dotted-decimal format.

Default

No remote IP address is defined.

Usage Guidelines

Use the **ip-address remote** command to configure the remote IP address of the tunnel peer. The remote address is considered to be the destination, while the local address is considered to be the source.

Use the **no** form of this command to remove the remote address configuration.

Examples

The following example configures the local and remote addresses for the `headquarters` IPSec tunnel peer:

```
[local]RedBack(config-context)#ipsec peer name headquarters
[local]RedBack(config-ipsec-peer)#ip-address local 10.1.1.2
[local]RedBack(config-ipsec-peer)#ip-address remote 20.2.1.1
```

Related Commands

ip-address local
ipsec peer name

ipsec key name

ipsec key name *key-name*

no ipsec key name *key-name*

Purpose

Creates a key structure and enters key configuration mode.

Command Mode

context configuration

Syntax Description

key-name	Name of the key structure you want to create or modify.

Default

If this command is not used, no key structures are configured.

Usage Guidelines

Use the **ipsec key name** command to add the named key structure into the database, and enter key configuration mode to configure the new key structure. You must create and configure any key referenced by the **ah hash**, **esp hash**, or **esp cipher** command in IPSec proposal configuration mode in this manner for the key to be valid.

Use the **no** form of this command to delete the named key structure from the database.

Examples

The following command creates a key structure called `key1` and enters key configuration mode:

```
[local]RedBack(config-ctx)#ipsec key name key1
[local]RedBack(config-ipsec-key)#
```

Related Commands

ah hash
esp cipher
esp hash
in
out
spi in
spi out

ipsec lifetime hard kbytes

ipsec lifetime hard kbytes *kbytes*

no ipsec lifetime hard kbytes

Purpose

Specifies the number of kilobytes of data transferred through an IP Security (IPSec) tunnel before the Security Association (SA) is deleted.

Command Mode

IPSec peer configuration

Syntax Description

kbytes	Number of kilobytes of data transferred before the SA is deleted. The default value is 2,000 kilobytes.

Default

The hard limit is 2,000 kilobytes.

Usage Guidelines

Use the **ipsec lifetime hard kbytes** command to set the hard limit in terms of kilobytes of data. Use the **ipsec lifetime hard seconds** command to set the hard limit in terms of time. If you have both in your configuration, the initiating peer starts dropping traffic when either hard limit is reached.

When a hard limit is reached, the initiating peer continues renegotiating for a new SA. The tunnel stays intact, but traffic intended for the tunnel is dropped.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets hard limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ipsec lifetime hard kbytes 6000
[local]RedBack(config-ipsec-peer)#ipsec lifetime hard seconds 3000
```

Related Commands

ipsec lifetime hard seconds
ipsec lifetime soft kbytes
ipsec lifetime soft seconds
ipsec peer name

ipsec lifetime soft kbytes

ipsec lifetime soft kbytes *kbytes*

no ipsec lifetime soft kbytes

Purpose

Specifies the number of kilobytes of data transferred through an IP Security (IPSec) tunnel before renegotiation for a new Security Association (SA) is started.

Command Mode

IPSec peer configuration

Syntax Description

kbytes	Number of kilobytes of data transferred before renegotiation is started. The default value is 1,800.

Default

The soft limit is 1,800 kilobytes.

Usage Guidelines

Use the **ipsec lifetime soft kbytes** command to set the soft limit in terms of kilobytes of data. Use the **ipsec lifetime soft seconds** command to set the soft limit in terms of time. If you have both in your configuration, the initiating peer begins the renegotiation when either soft limit is reached.

When a soft limit is reached, the initiating peer begins renegotiating for a new SA. The tunnel stays intact and secure traffic continues to be passed through the tunnel.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets soft limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ipsec lifetime soft kbytes 3000
[local]RedBack(config-ipsec-peer)#ipsec lifetime soft seconds 2000
```

Related Commands

ipsec lifetime hard kbytes
ipsec lifetime hard seconds
ipsec lifetime soft seconds
ipsec peer name

ipsec lifetime hard seconds

ipsec lifetime hard seconds *seconds*

no ipsec lifetime hard seconds

Purpose

Specifies the number of seconds from creation of the Security Association (SA) before the SA is deleted.

Command Mode

IPSec peer configuration

Syntax Description

seconds	Number of seconds from creation of the SA before it is deleted. The default value is 3,600.

Default

The hard limit is 3,600 seconds.

Usage Guidelines

Use the **ipsec lifetime hard seconds** command to set the hard limit in terms of time. Use the **ipsec lifetime hard kbytes** command to set the hard limit in terms of kilobytes of data. If you have both in your configuration, the initiating peer starts dropping traffic when either hard limit is reached.

When a hard limit is reached, the initiating peer continues renegotiating for a new SA. The tunnel stays intact, but traffic intended for the tunnel is dropped.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets hard limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ipsec lifetime hard kbytes 6000
[local]RedBack(config-ipsec-peer)#ipsec lifetime hard seconds 3000
```

Related Commands

ipsec lifetime hard kbytes
ipsec lifetime soft kbytes
ipsec lifetime soft seconds
ipsec peer name

ipsec lifetime soft seconds

ipsec lifetime soft seconds *seconds*

no ipsec lifetime soft seconds

Purpose

Specifies the number of seconds from creation of the Security Association (SA) before renegotiation for a new SA is started.

Command Mode

IPSec peer configuration

Syntax Description

seconds	Number of seconds from creation of the SA before renegotiation begins. The default value is 3,240 seconds.

Default

The soft limit is 3,240 seconds.

Usage Guidelines

Use the **ipsec lifetime soft seconds** command to set the soft limit in terms of time. Use the **ipsec lifetime soft kbytes** command to set the soft limit in terms of kilobytes of data. If you have both in your configuration, the initiating peer begins the renegotiation when either soft limit is reached.

When a soft limit is reached, the initiating peer begins renegotiating for a new SA. The tunnel stays intact and secure traffic continues to be passed through the tunnel.

Use the **no** form of this command to remove the limit from the configuration.

Examples

The following example sets soft limits for both time and kilobytes of data:

```
[local]RedBack(config-ipsec-peer)#ipsec lifetime soft kilobytes 30000
[local]RedBack(config-ipsec-peer)#ipsec lifetime soft seconds 1800
```

Related Commands

ipsec lifetime hard kbytes
ipsec lifetime hard seconds
ipsec lifetime soft kbytes
ipsec peer name

ipsec mode

ipsec mode {**main** | **aggressive**}

no ipsec mode

Purpose

Specifies the mode to be used when negotiating Internet Security Association and Key Management Protocol (ISAKMP) for both IP Security (IPSec) and Internet key exchange (IKE).

Command Mode

IPSec peer configuration

Syntax Description

main	Specifies that main ISAKMP mode is to be used.
aggressive	Specifies that aggressive ISAKMP mode is to be used.

Default

Main ISAKMP mode is used.

Usage Guidelines

Use the **ipsec mode** command to specify the mode to be used when negotiating ISAKMP. ISAKMP is a negotiation protocol with two possible modes—main and aggressive. Support for these modes is implemented in accordance with RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*.

Use the **no** form of this command to revert to the default (main) mode.

Examples

The following example configures aggressive ISAKMP mode for the peer:

```
[local]RedBack(config-ipsec-peer)#ipsec mode aggressive
```

Related Commands

ipsec peer name

ipsec options

ipsec options pfs

no ipsec options pfs

Purpose

Enables the specified IP Security (IPSec) options.

Command Mode

IPSec peer configuration

Syntax Description

pfs	Specifies that Perfect Forward Secrecy (PFS) is to be enabled. Currently, this is the only IPSec option supported.

Default

PFS is disabled.

Usage Guidelines

Use the **ipsec options** command to enable PFS. PFS is implemented in accordance with RFC 2409, *The Internet Key Exchange (IKE)*. At this time, PFS is the only IPSec option supported by the Access Operating System (AOS).

Use the **no** form of this command to disable PFS.

Examples

The following example enables PFS for a peer:

```
[local]RedBack(config-ipsec-peer)#ipsec options pfs
```

Related Commands

ipsec peer name

ipsec peer default

ipsec peer default

no ipsec peer default

Purpose

Enters IP Security (IPSec) peer configuration mode to change the factory default settings that are applied to new IPSec peers.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

If this command is not used, no default IPSec peer is configured.

Usage Guidelines

Use the **ipsec peer default** command to enter IPSec peer configuration mode so you can change the default configuration for new IPSec peers. The configuration settings of individual peers override the new default settings, just as they would if the factory default settings remained unchanged. See the "Configuring IPSec" chapter in the *Access Operating System (AOS) Configuration Guide* for a table listing the factory default settings.

Only one set of defaults can be configured per context. Once this new default configuration has been established, all new IPSec peers adopt the new settings, unless changed within the configuration of individual peers.

Use the **no** form of this command to return the initial settings for new IPSec peers to the factory defaults.

Examples

The following example shows changing IPSec peer default settings from the factory defaults:

```
[local]RedBack(config-ctx)#ipsec peer default
[local]RedBack(config-ipsec-peer)#ipsec mode aggressive
[local]RedBack(config-ipsec-peer)#ipsec pfs-group 2
[local]RedBack(config-ipsec-peer)#ike group 2
```

Related Commands

debug ipsec peer
ipsec peer name
show ipsec peer
show ipsec stats

ipsec peer name

ipsec peer name *peer-name*

no ipsec peer name *peer-name*

Purpose

Creates an IP Security (IPSec) peer and enters IPSec peer configuration mode.

Command Mode

context configuration

Syntax Description

peer-name	Name of the IPSec peer you want to create or modify.

Default

If this command is not used, no IPSec peers are configured.

Usage Guidelines

Use the **ipsec peer name** command to add the named IPSec peer into the database and enter IPSec peer configuration mode so you can configure the new peer.

Use the **no** form of this command to delete the named peer from the database.

Examples

The following example creates a peer called `corporate` and enters IPSec peer configuration mode:

```
[local]RedBack(config-ctx)#ipsec peer name corporate
[local]RedBack(config-ipsec-peer)#
```

Related Commands

debug ipsec peer
ipsec peer default
show ipsec peer
show ipsec stats

ipsec pfs-group

ipsec pfs-group *group-num*

[**no** | **default**] **ipsec pfs-group**

Purpose

Specifies the Internet Security Association and Key Management Protocol (ISAKMP) group that is to be used by the Diffie-Hellman key exchange to construct key material for an IP Security (IPSec) Security Association (SA).

Command Mode

IPSec peer configuration

Syntax Description

group-num Valid ISAKMP group numbers are 1 through 5 as follows:

1 = 768-bit modular exponentiation group (MODP) group
2 = 1024-bit MODP group
3 = Galois Field (GF)[2^{155}] group
4 = GF[2^{185}] group
5 = 1536-bit MODP group

Default

ISAKMP group number 1 is used.

Usage Guidelines

Use the **ipsec pfs-group** command only if the Perfect Forward Secrecy (PFS) option has been enabled using the **ipsec options** command. If PFS has been enabled, the **ipsec pfs-group** command is required.

Use the **no** or **default** form of this command to revert to the default group number 1.

Examples

The following example selects `ISAKMP group 4` for purposes of constructing key material:

```
[local]RedBack(config-ipsec-peer)#ipsec options pfs
[local]RedBack(config-ipsec-peer)#ipsec pfs-group 4
```

Related Commands

ipsec options
ipsec peer name

ipsec policy name

ipsec policy name *pol-name*

no ipsec policy name *pol-name*

Purpose

Creates an IP Security (IPSec) policy and enters IPSec policy configuration mode.

Command Mode

context configuration

Syntax Description

pol-name	Name of the IPSec policy you want to create or modify.

Default

If this command is not used, no IPSec policies are configured.

Usage Guidelines

Use the **ipsec policy name** command to add the named IPSec policy into the database and enter IPSec policy configuration mode so you can configure the new policy. You must create and configure any policy referenced by the **ipsec tunnel policy** command in this manner for the policy to be valid.

Use the **no** form of this command to delete the named policy from the database.

Examples

The following command creates a policy called `telecommuter1` and enters IPSec policy configuration mode:

```
[local]RedBack(config-ctx)#ipsec policy name telecommuter1
[local]RedBack(config-ipsec-policy)#
```

Related Commands

ipsec tunnel policy
tunnel ip

ipsec proposal crypto name

ipsec proposal crypto name *prop-name*

no ipsec proposal crypto name *prop-name*

Purpose

Creates an IP Security (IPSec) proposal and enters IPSec proposal configuration mode.

Command Mode

context configuration

Syntax Description

prop-name	Name of the IPSec proposal you want to create or modify.

Default

If this command is not used, no IPSec proposals are configured.

Usage Guidelines

Use the **ipsec proposal crypto name** command to add the named IPSec proposal into the database and enter IPSec proposal configuration mode so you can configure the new proposal. You must create and configure any proposal referenced by the **proposal crypto** command in this manner for the proposal to be valid. Use this command to create manual proposals. Use the **ipsec proposal ike name** command to create Internet key exchange (IKE)-negotiated proposals.

Use the **no** form of this command to delete the named proposal from the database.

Examples

The following command creates a manual proposal called `testing` and enters IPSec proposal configuration mode:

```
[local]RedBack(config-ctx)#ipsec proposal name testing
[local]RedBack(config-ipsec-proposal)#
```

Related Commands

proposal crypto

ipsec proposal ike name

ipsec proposal ike name *ike-name*

no ipsec proposal ike name *ike-name*

Purpose

Creates an Internet key exchange (IKE) proposal and enters IKE proposal configuration mode.

Command Mode

context configuration

Syntax Description

ike-name	Name of the IKE proposal you want to create or modify.

Default

If this command is not used, no IKE proposals are configured.

Usage Guidelines

Use the **ipsec proposal ike name** command to add the named IPSec proposal into the database and enter IPSec proposal configuration mode so you can configure the new proposal. You must create and configure any proposal referenced by the **proposal ike** command in this manner for the proposal to be valid. Use this command to create IKE-negotiated proposals. Use the **ipsec proposal crypto name** command to create manual proposals.

Use the **no** form of this command to delete the named proposal from the database.

Examples

The following command creates an IKE-negotiated proposal called `onceonly` and enters IKE proposal configuration mode:

```
[local]RedBack(config-ctx)#ipsec proposal ike name onceonly
[local]RedBack(config-ipsec-proposal_ike)#
```

Related Commands

proposal ike

ipsec tunnel policy

ipsec tunnel policy *pol-name*

no ipsec tunnel policy *pol-name*

Purpose

Binds a subscriber to an IP Security (IPSec) policy.

Command Mode

subscriber configuration

Syntax Description

pol-name	Name of the IPSec policy to which the subscriber is to be bound.

Default

If this command is not used, the subscriber is not bound to an IPSec policy.

Usage Guidelines

Use the **ipsec tunnel policy** command to bind a subscriber to an IPSec policy. Any traffic from the subscriber that matches a policy entry is tunneled through the IPSec peer defined in the policy configuration. All other traffic is routed normally. Any traffic destined to this subscriber that matches the reverse of the policy entry must have originated from the IPSec peer associated with the policy entry.

If a subscriber configuration calls for binding to both an IPSec policy and an IPSec peer, the binding to the policy takes precedence.

Use the **no** form of this command to remove the binding.

Examples

The following example binds a subscriber named `jack` to an IPSec policy named `main`:

```
[local]RedBack(config)#subscriber jack
[local]RedBack(config-sub)#ipsec tunnel policy main
```

Related Commands

ipsec policy name
tunnel ip

out

out {**string** *string* | **hex** *binary*}

[**no**] **out**

Purpose

Defines the key used for the outbound Security Association (SA) of a manual tunnel.

Command Mode

IPSec key configuration

Syntax Description

string *string*	Key to be used for the outbound SA of a manual tunnel. The **string** keyword is followed by an ASCII string.
hex *binary*	Key to be used for the outbound SA of a manual tunnel. The **hex** keyword is followed by a hexadecimal string.

Default

No key is defined for the outbound SA.

Usage Guidelines

Use the **out** command only for tunnels using manual proposals. The key can be expressed either as an ASCII string or as a hexadecimal string.

Use the **no** form of this command to remove the key definition from the configuration.

Examples

The following example defines inbound and outbound keys:

```
[local]RedBack(config-ctx)#ipsec key name perfect
[local]RedBack(config-ipsec-key)#in string 494949jjf8fuueeeoo
[local]RedBack(config-ipsec-key)#out string 33jmdiid999fff
```

Related Commands

in
ipsec key name
spi in
spi out

port te

port te *slot/port*

Purpose

Enters port configuration mode for the specified port.

Command Mode

global configuration

Syntax Description

slot/port	Backplane slot number and port number of the port to be configured.

Default

None

Usage Guidelines

Use the **port te** command to enter port configuration mode. Upon system initialization, all physical ports are automatically recognized and the appropriate port command is made available in the command-line interface (CLI).

Examples

The following example selects the IPSec/Compression Transform Engine (TE) port in slot 4 of the chassis and enters port configuration mode. The port is subsequently enabled using the **no shutdown** command.

```
[local]RedBack(config)#port te 4/0
[local]RedBack(config-port)#no shutdown
```

Related Commands

shutdown

proposal crypto

proposal crypto *prop-name*

no proposal crypto *prop-name*

Purpose

Specifies an IP Security (IPSec) proposal that can be used with this peer.

Command Mode

IPSec peer configuration

Syntax Description

prop-name	Name of the IPSec proposal being associated with the peer.

Default

No IPSec proposals are specified for the peer.

Usage Guidelines

Use the **proposal crypto** command to add one or more proposals to the IPSec peer configuration. In the case of manual proposals, only one proposal is needed or used, and it must contain references to an IPSec key. In the case of Internet key exchange (IKE) proposal negotiation, multiple proposals can be considered for use. The proposals are negotiated with the remote peer in the order in which they are configured. The first proposal successfully negotiated is the one used.

Use the **no** form of this command to disassociate the proposal from the peer.

Examples

The following example creates three proposals for the IPSec peer named `topsecurity`. If manual proposals are used, only the first configured proposal is relevant. If IKE proposal negotiation is used, the proposals are considered for use in the order in which they appear in the configuration.

```
[local]RedBack(config-ctx)#ipsec peer name topsecurity
[local]RedBack(config-ipsec-peer)#proposal crypto x24end
[local]RedBack(config-ipsec-peer)#proposal crypto x24mid
[local]RedBack(config-ipsec-peer)#proposal crypto x24start
```

Related Commands

ipsec peer name
proposal ike

proposal ike

proposal ike *prop-name*

no proposal ike *prop-name*

Purpose

Specifies an Internet key exchange (IKE) proposal that can be used with this peer.

Command Mode

IPSec peer configuration

Syntax Description

prop-name	Name of the IKE proposal being associated with the peer.

Default

No IKE proposals are specified for the peer.

Usage Guidelines

Use the **proposal ike** command to add one or more IKE proposals to a peer configuration. IKE proposals are used to negotiate a Security Association (SA). Once the SA has been established, the two peers use IKE to negotiate a proposal from among those configured for the peer. Typically, multiple IKE proposals are configured for a peer to ensure that a match can be found with which to establish the SA.

Use the **no** form of this command to disassociate the IKE proposal from the peer.

Examples

The following example creates three IKE proposals for the IP Security (IPSec) peer named `corporate`:

```
[local]RedBack(config-ctx)#ipsec peer name corporate
[local]RedBack(config-ipsec-peer)#proposal ike prop1
[local]RedBack(config-ipsec-peer)#proposal ike prop2
[local]RedBack(config-ipsec-peer)#proposal ike prop3
```

Related Commands

ipsec peer name
proposal crypto

show ipsec peer

show ipsec peer {**name** *peer-name* | **tunnel-id** *tunnel-id*}

Purpose

Displays the status of the specified IP Security (IPSec) tunnel.

Command Mode

administrator exec

Syntax Description

name *peer-name*	Specific IPSec tunnel peer about which you want status information.
tunnel-id *tunnel-id*	Numeric tunnel ID (available in the **show ipsec peer** command output) for the IPSec tunnel about which you want status information.

Default

If no optional construct is used, this command displays the status of all IPSec tunnel peers.

Usage Guidelines

Use the **show ipsec peer** command to display status information about the IPSec tunnel. Whether you use the **name** *peer-name* construct, or the **tunnel-id** *tunnel-id* construct, the following information is displayed about the specified peer (tunnel):

Table 27-1 Output When a Peer (Tunnel) is Specified

Field	Description
Tunnel name	Name given to the peer using the **ipsec peer** name command.
Tunnel-ID	Numeric ID of the peer (tunnel), device-wide—automatically assigned. This ID can be used in the **show ipsec peer** and **show ipsec stats** commands
TE Tunnel-ID	Numeric ID of the peer within the IPSec/Compression Transform Engine module—automatically assigned.
TE port	Slot/port designation.
Tunnel-state	Indicates if the tunnel is up.
Tunnel-uptime	Number of seconds the tunnel has been up if the Tunnel-state is UP.

Table 27-1 Output When a Peer (Tunnel) is Specified

Field	Description
Tunnel-Scr-IP	Source IP address of the tunnel.
Tunnel-Dst-IP	Destination IP address of the tunnel.
Decode-encaps	Encapsulation mode for the inbound traffic.
Encode-encaps	Encapsulation mode for the outbound traffic.
Decode-ah-mac	Hash algorithm of the authentication header (AH) for inbound traffic.
Encode-ah-mac	Hash algorithm of the authentication header (AH) for outbound traffic.
Decode-esp-mac	Hash algorithm of the Encapsulating Security Payload (ESP) for inbound traffic.
Encode-esp-mac	Hash algorithm of the Encapsulating Security Payload (ESP) for outbound traffic.
Decode-esp-cipher	Cipher algorithm of the Encapsulating Security Payload (ESP) for inbound traffic.
Encode-esp-cipher	Cipher algorithm of the Encapsulating Security Payload (ESP) for inbound traffic.

Examples

The following example uses the **show ipsec peer** command to display information about the specified tunnel peer:

```
[local]RedBack#show ipsec peer name jackson1

Tunnel name: jackson1
Tunnel-ID: 3                          TE Tunnel-ID: 2
TE port: 4/0
Tunnel-state: UP                      Tunnel-uptime 0
Tunnel-Src-IP: 34.34.11.10            Tunnel-Dst-IP 126.34.11.10
Decode-encaps: TUNNEL                 Encode-encaps: TUNNEL
Decode-ah-mac: none                   Encode-ah-mac: none
Decode-esp-mac: sha-96                Encode-esp-mac: sha-96
Decode-esp-cipher: des-cbc            Encode-esp-cipher: des-cbc
```

Related Commands

show ipsec stats

show ipsec stats

show ipsec stats {**global** | **name** *peer-name* | **tunnel-id** *tunnel-id*}

Purpose

Displays counters and statistics related to all, or a specified IP Security (IPSec) tunnel.

Command Mode

administrator exec

Syntax Description

global	Specifies that only transmit and receive counters for IPSec/Compression Transform Engine (TE) modules are to be displayed.
name *peer-name*	Name of the IPSec tunnel peer that identifies the tunnel about which you want detailed information.
tunnel-id *tunnel-id*	Numeric tunnel ID (available in the **show ipsec peer** command output) of the IPSec tunnel about which you want detailed information.

Default

If no optional construct is used, the **show ipsec stats** command displays detailed information for all IPSec tunnels in the current context.

Usage Guidelines

Use the **show ipsec stats** command to display counters and statistics related to one or all IPSec tunnels. When you use the **global** keyword, the following information is displayed about each peer:

Table 27-2 Output When a Peer is Specified

Field	Description
TE port	Slot/port designation
RX IKE packets	IKE packets received
TX IKE packets	IKE packets transmitted

When you use the **name** *peer-name* construct, or the **tunnel-id** *tunnel-id* construct, the following information is displayed about the specified peer:

Table 27-3 Output When a Peer (Tunnel) is Specified

Field	Description
Tunnel name	Name given to the peer using the **ipsec peer** name command.
Tunnel-ID	Numeric ID of the peer (tunnel), device-wide—automatically assigned. This ID can be used in the **show ipsec peer** and **show ipsec stats** commands.
TE Tunnel-ID	Numeric ID of the peer within the IPSec/Compression Transform Engine module—automatically assigned.
TE port	Slot/port designation.
Decode-pkts	Number of inbound packets.
Decode-bytes	Total bytes in inbound packets.
Decode-sa-uptime	Number of seconds the inbound SA has been up.
Decode-dropped	Number of inbound packets dropped.
Decode-ah-icv-fail	Number of encryption check failures on inbound packets (AH error).
Decode ah-replay	Number of AH replay errors (same packet sent multiple times) on inbound traffic.
Decode-esp-icv-fail	Number of encryption check failures on inbound packets (ESP error).
Decode-esp-replay	Number of ESP replay errors on inbound traffic.
ESP decrypt-failures	Number of ESP decryption failures.
Encode-pkts	Number of outbound packets.
Encode-bytes	Total bytes in outbound packets.
Encode-sa-uptime	Number of seconds the outbound SA has been up.
Encode-dropped	Number of outbound packets dropped.
Encode-ah-icv-fail	Number of encryption check failures on outbound packets (AH error).
Encode ah-replay	Number of AH replay errors (same packet sent multiple times) on outbound traffic.
Encode-esp-icv-fail	Number of encryption check failures on outbound packets (ESP error).
Encode-esp-replay	Number of ESP replay errors on outbound traffic.
ESP decrypt-failures	Number of ESP decryption failures.

Examples

The following example uses the **show ipsec stats** command with the **global** keyword to display receive and transmit counters for all TE ports:

```
[local]RedBack#show ipsec stats global

TE port: 4/0
  RX IKE packets: 0
  TX IKE packets: 0
TE port: 4/1
  RX IKE packets: 0
  TX IKE packets: 0
```

The following example uses the **show ipsec stats** command to display detailed statistics for a specific peer (tunnel):

```
[local]RedBack#show ipsec stats name whaling

Tunnel name: whaling
Tunnel-ID: 1                    TE Tunnel-ID: 0
TE port: 4/0
Decode-pkts: 11                 Encode-pkts: 12
Decode-bytes: 11792             Encode-bytes: 12336
Decode-sa-uptime: 0             Encode-sa-uptime: 0
Decode-dropped: 0               Encode-dropped: 0
Decode-ah-icv-fail: 0           Encode-ah-icv-fail: 0
Decode-ah-replay: 0             Encode-ah-replay: 0
Decode-esp-icv-fail: 0          Encode-esp-icv-fail: 0
Decode-esp-replay: 0            Encode-esp-replay: 0
ESP decrypt-failures: 0
```

Related Commands

show ipsec peer

show te cpu

show te cpu

Purpose

Displays CPU utilization statistics relevant to the IPSec/Compression Transform Engine (TE) ports.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show te cpu** command to display CPU utilization statistics for TE ports. The following information is displayed for each TE port when you use the **show te cpu** command:

Table 27-4 CPU Utilization

Field	Description
TE port	Slot/port designation
user	Percentage of CPU being used by the IPSec software
idle	Percentage of CPU not being used
system	Percentage of CPU being used by the system for overhead tasks, outside of the IPSec software

Examples

The following example uses the **show te cpu** command to display CPU utilization statistics for all TE ports:

```
[local]RedBack#show te cpu

TE port: 4/0
  utilization 159 (user) / -59 (idle) / 0 (system)
TE port: 4/1
  utilization 158 (user) / -58 (idle) / 0 (system)
```

Related Commands

show te performance
show te ps
show te time

show te performance

show te performance

Purpose

Displays performance statistics relevant to the IPSec/Compression Transform Engine (TE) ports.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show te performance** command to display performance statistics for TE ports.

Examples

The following example requests performance statistics for all TE ports:

```
[local]RedBack#show te performance
```

Related Commands

show te cpu
show te ps
show te time

show te ps

show te ps

Purpose

Displays information about processes relevant to the IPSec/Compression Transform Engine (TE) ports.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show te processes** command to display process information related to TE ports.

Examples

The following example requests information about processes related to TE ports:

```
[local]RedBack#show te ps

TE port: 2/0
  NAME         COUNT      MAX_MSEC  AVG_MSEC  MAX_WAIT  AVG_WAIT  CPU
  ------------ -----      --------  --------  --------  --------  -----
  80012F1C     2          1         1         15        13        0
  800109E4     20674886   90        -1        3         0         47
  usleep       20674812   0         -1        0         0         52
  800B9D60     6          0         0         0         0         0
  8004C578     110        0         0         0         0         0
  80042974     1          0         0         0         0         0

TE port: 2/1
  NAME         COUNT      MAX_MSEC  AVG_MSEC  MAX_WAIT  AVG_WAIT  CPU
  ------------ -----      --------  --------  --------  --------  -----
  80012F1C     2          1         1         15        13        0
  800109E4     20581674   12        -1        3         0         47
  usleep       20581598   0         -1        0         0         52
```

```
800B9D60     6          0          0          0          0          0
8004C578     110        0          0          0          0          0
```

Related Commands

show te cpu
show te performance
show te time

show te time

show te time

Purpose

Displays the amount of time each IPSec/Compression Transform Engine (TE) port has been running.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show te time** command to display the amount of time that each IPSec/Compression TE port has been running.

Examples

The following example uses the **show te time** command to display the amount of time that each TE port has been running:

```
[local]RedBack#show te time

TE port: 4/0
  current time = 19936 seconds 562806 useconds
TE port: 4/1
  current time = 19918 seconds 794200 useconds
```

Related Commands

show te performance
show te ps
show te cpu

spi in

spi in *num*

[**no**] **spi in**

Purpose

Defines the Security Parameter Index (SPI) used for the inbound Security Association (SA) of a manual tunnel.

Command Mode

IPSec key configuration

Syntax Description

num	SPI for the inbound SA. The range of values is 1 to 65,535.

Default

No SPI is defined for the inbound SA.

Usage Guidelines

Use the **spi in** command only for tunnels using manual proposals.

Use the **no** form of this command to remove the SPI from the configuration.

Examples

The following example establishes SPIs for a key called `perfect`:

```
[local]RedBack(config-ctx)#ipsec key name perfect
[local]RedBack(config-ipsec-key)#spi in 10001
[local]RedBack(config-ipsec-key)#spi out 10011
```

Related Commands

in
ipsec key name
out
spi out

spi out

spi out *num*

[**no**] **spi out**

Purpose

Defines the Security Parameter Index (SPI) used for the outbound Security Association (SA) of a manual tunnel.

Command Mode

IPSec key configuration

Syntax Description

num	SPI for the outbound SA. The range of values is 1 to 65,535.

Default

No SPI is defined for the outbound SA.

Usage Guidelines

Use the **spi out** command only for tunnels using manual proposals.

Use the **no** form of this command to remove the SPI from the configuration.

Examples

The following example establishes SPIs for a key called `perfect`:

```
[local]RedBack(config-ctx)#ipsec key name perfect
[local]RedBack(config-ipsec-key)#spi in 10001
[local]RedBack(config-ipsec-key)#spi out 10011
```

Related Commands

in
ipsec key name
out
spi in

tunnel ip

tunnel ip *src-addr src-netmask dst-addr dst-netmask* **name** *peer-name*

no tunnel ip *src-addr src-netmask dst-addr dst-netmask* **name** *peer-name*

Purpose

Specifies the range of IP addresses to match against packets arriving from or destined to a subscriber and specifies the IP Security (IPSec) peer to be used for all traffic that matches the IP address criteria.

Command Mode

IPSec policy configuration

Syntax Description

src-addr	Source IP address of packets arriving from and destined for the subscriber; expressed in the form A.B.C.D.
src-netmask	Indication of which bits in the *src-addr* argument are significant for purposes of matching; expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the netmask mean that the corresponding bits in the *src-addr* argument must match; one-bits in the netmask mean that the corresponding bits in the *src-addr* argument are ignored.
dst-addr	Destination IP address of packets arriving from and destined for the subscriber; expressed in the form A.B.C.D.
dst-netmask	Indication of which bits in the *dst-addr* argument are significant for purposes of matching; expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the netmask mean that the corresponding bits in the *dst-addr* argument must match; one-bits in the netmask mean that the corresponding bits in the *dst-addr* argument are ignored.
name *peer-name*	Name of the IPSec tunnel peer to be used when the IP source or destination address matches the specified criteria.

Default

If the subscriber is bound to an IPSec policy and the **tunnel ip** command is not used, all traffic to and from the subscriber is routed normally.

Usage Guidelines

Use the **tunnel ip** command to specify which traffic to or from a policy-bound subscriber should be treated as secure and which should not. Traffic that matches the IP address requirements in either direction is treated as secure and is passed through the specified IPSec tunnel peer. All traffic that does not match the IP address requirements is routed normally.

Although you enter this command as if the subscriber is the source, the IP address requirements specified are applied in both directions—both to and from the subscriber.

If a packet destined for the subscriber matches the IP address specifications, but did not originate from the specified IPSec tunnel peer, the packet is dropped. Secure traffic must stay within the IPSec tunnel.

You can use this command multiple times in a policy configuration, specifying how different types of secure traffic are to be handled.

Use the **no** form of this command to remove the specification from the configuration.

Examples

The following example configures a policy with specifications for handling three different types of secure traffic:

```
[local]RedBack(config-ctx)#ipsec policy name headquarters
[local]RedBack(config-ipsec-policy)#tunnel ip 10.25.0.0 0.0.255.255 10.10.0.0
0.0.255.255 name headquarters
[local]RedBack(config-ipsec-policy)#tunnel ip 20.1.1.1 0.0.255.255 10.20.0.0
0.0.255.255 name all
[local]RedBack(config-ipsec-policy)#tunnel ip 10.25.0.0 0.0.255.255 10.30.0.0
0.0.255.255 name sales
```

Related Commands

ipsec policy name

Part 8

IP Services

DNS Commands

This chapter describes the commands used to configure Domain Name System (DNS) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure DNS features, and configuration examples, see the "Configuring DNS" chapter in the *Access Operating System (AOS) Configuration Guide*.

clear ip localhosts

clear ip localhosts [*hostname*]

Purpose

Deletes hostname-to-IP address mappings stored in the local host table.

Command Mode

administrator exec

Syntax Description

hostname	Optional. Specific hostname to be deleted.

Usage Guidelines

Use the **clear ip localhosts** command to delete hostname-to-IP address mappings stored in the local host table. Using this command without the optional *hostname* argument clears the entire local host table.

When you specify a specific hostname using the *hostname* argument, only the single entry matching the hostname is deleted.

Examples

The following example deletes all hostname-to-IP address mappings:

```
[local]RedBack#clear ip localhosts
```

Related Commands

ip localhost
show ip localhosts

debug ip dns

debug ip dns

no debug ip dns

Purpose

Enables the logging of Domain Name System (DNS) debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip dns** command to enable DNS debugging. When debugging is enabled, DNS messages are logged. Use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable DNS debugging.

Examples

The following example enables debug logging for DNS:

```
[local]RedBack#debug ip dns
```

Related Commands

dns
ip domain-lookup
ip domain-name

ip name-servers
logging console
show debugging
terminal monitor

dns

dns {**primary** | **secondary**} *address*

no dns {**primary** | **secondary**} *address*

Purpose

Configures the IP address of a primary and secondary Domain Name System (DNS) server that a subscriber should use.

Command Mode

subscriber configuration

Syntax Description

primary	Specifies that the DNS server should be used as the primary server.
secondary	Specifies that the DNS server should be used as the secondary server.
address	IP address of a DNS server.

Default

DNS server information is not provided to the subscriber.

Usage Guidelines

Use the **dns** command to configure the IP address of a primary and secondary DNS server that a subscriber should use. This command does not instruct the Subscriber Management System (SMS) device to use the specified name servers in any way for its own purposes. Rather, this information is passed to the subscriber via either Point-to-Point Protocol (PPP) negotiation. The subscriber uses DNS to resolve IP addresses from hostnames. These values are utilized via PPP when the remote peer requests this information (see RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*). The SMS device does not push this information to the remote peer.

Use the **no** form of this command to remove the DNS server information from a subscriber record.

Examples

The following example provides the primary DNS server address, `10.2.3.4`, to a subscriber named `kenny`:

```
[local]RedBack(config-ctx)#subscriber name kenny
[local]RedBack(config-sub)#dns primary 10.2.3.4
```

Related Commands

bind authentication
bind subscriber
subscriber

ip dns-ttl

ip dns-ttl *timeout*

no ip dns-ttl

Purpose

Specifies the timeout in seconds for Domain Name System (DNS) entries in the DNS cache table.

Command Mode

context configuration

Syntax Description

timeout	Number of seconds for which DNS entries remain in the cache table. The range of values is 0 to 172,800.

Default

Entries remain in the cache table for 3,600 seconds.

Usage Guidelines

Use the **ip dns-ttl** command to specify the timeout value for DNS entries in the DNS cache table. The hostnames that are resolved by DNS are cached in the IP localhosts table until the timeout is expired. The hostname, its IP address, and the timeout value as defined by the *timeout* argument in the **ip dns-ttl** command are displayed by the **show ip localhosts** command.

Use the **no** form of this command to set the timeout value to the default of 3,600 seconds.

Examples

The following example configures DNS entries to remain in the cache table for 5,000 seconds:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip dns-ttl 5000
```

Related Commands

show ip localhosts

ip domain-lookup

ip domain-lookup

no ip domain-lookup

Purpose

Configures the Subscriber Management System (SMS) device to use Domain Name System (DNS) resolution to look up hostname-to-IP address mappings in the host table for the context.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

DNS lookup is disabled.

Usage Guidelines

Use the **ip domain-lookup** command to configure the SMS device to use DNS resolution to look up hostname-to-IP address mappings in the host table for the context. DNS resolution translates, or maps, hostnames to IP addresses, allowing an administrator to ping or Telnet to a host using a hostname, instead of having to know the host's specific IP address. When an Access Operating System (AOS) command references a hostname, the SMS device consults the local host table to obtain the hostname-to-IP address mapping. If the information is not in the local host table, the SMS device generates a DNS query to resolve the hostname.

For DNS resolution to function, DNS servers must also be configured using the **ip name-servers** command. Hostnames that are statically entered into the local host table via the **ip localhost** command can also be used in DNS resolution.

Use the **no** form of this command to disable DNS resolution lookup for the context.

Examples

The following example enables DNS resolution for the local context:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip domain-lookup
```

Related Commands

ip domain-name
ip localhost
ip name-servers

ip domain-name

ip domain-name *dom-name*

no ip domain-name *dom-name*

Purpose

Specifies the Domain Name System (DNS) name for the context.

Command Mode

context configuration

Syntax Description

dom-name	Name of the domain.

Default

No DNS name is configured for the context.

Usage Guidelines

Use the **ip domain-name** command to specify the DNS name for the context. One domain name per context is supported.

Use the **no** form of this command to remove the DNS name for the context.

Examples

The following example specifies that the domain name for the current context is `redback.com`:

```
[local]RedBack(config-ctx)#ip domain-name redback.com
```

Related Commands

ip domain-lookup
ip name-servers

ip localhost

ip localhost *hostname ip-address*

no ip localhost *hostname ip-address*

Purpose

Statically configures hostname-to-IP address Domain Name System (DNS) mappings in the Subscriber Management System (SMS) device host table for the context.

Command Mode

context configuration

Syntax Description

hostname	Name of the host.
ip-address	IP address of the host.

Default

No hostname-to-IP address mapping is specified for the context.

Usage Guidelines

Use the **ip localhost** command to statically configure hostname-to-IP address DNS mappings in the SMS device host table for the context. The SMS device always consults the host table prior to generating a DNS lookup query. Entries created with the **ip localhost** command are never aged out. Specifying a new IP address for an existing hostname removes the previously configured IP address.

Use the **no** form of this command to remove the specified static entry.

Examples

The following example statically maps the hostname `charon` to the IP address of `10.10.13.24` for the `local` context:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip localhost charon 10.10.13.24
```

Related Commands

ip domain-lookup
ip domain-name
ip name-servers

ip name-servers

ip name-servers *ip-address* [*ip-address*]

no ip name-servers

Purpose

Configures a primary and, optionally, a secondary Domain Name System (DNS) server to be used by the Subscriber Management System (SMS) device.

Command Mode

context configuration

Syntax Description

ip-address	IP address of a primary, and optionally a secondary, DNS server.

Default

None

Usage Guidelines

Use the **ip name-servers** command to configure a primary and, optionally, a secondary DNS server to be used by the SMS device. You can configure a maximum of two DNS servers. DNS servers are queried in the order specified: primary followed by secondary. For DNS resolution to function, you must also use the **ip domain-lookup** command to configure domain-name lookup. There must be a route to the DNS servers in the IP routing table.

Use the **no** form of this command to remove the specified DNS server association from the context. If the primary DNS server is deleted, any configured secondary DNS server becomes the primary server. Entering a new **ip name-servers** command overrides the previously configured information.

Examples

The following example configures an association with a primary DNS server at IP address `128.215.33.47`, and a secondary server at IP address `196.145.92.33` for the `local` context:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip name-servers 128.215.33.47 196.145.92.33
```

The following example removes the secondary DNS server:

```
[local]RedBack(config-ctx)#no ip name-servers 196.145.92.33
```

Related Commands

ip domain-lookup
ip domain-name
ip localhost

show ip localhosts

show ip localhosts [*hostname*]

Purpose

Displays hostname-to-IP address mappings stored in the local host table for the context.

Command Mode

operator exec

Syntax Description

hostname	Optional. Name of the host.

Default

Lists all hostname-to-IP address mappings stored in the local host table in the current context.

Usage Guidelines

Use the **show ip localhosts** command to display hostname-to-IP address mappings stored in the local host table for the context. When the optional hostname argument is not specified, this command lists all hostname-to-IP address mappings stored in the local host table for the context. When you specify a hostname using the *hostname* argument, just the single entry matching the specified hostname is displayed.

Examples

The following example shows sample output from the **show ip localhosts** command. `Static`, in the Type field, indicates that the entry was created statically. `Learned` indicates that the corresponding entries were inserted by the Domain Name System (DNS):

```
[local]RedBack>show ip localhosts

Host Name               IP Address       Type        TTL
unitone.companya.com    122.53.199.199   learned     5000
unittwo.companyb.com    122.33.44.5      learned     3600
temphost                172.2.3.1        static      0
```

As shown in this example, static entries always have a timeout value (`TTL`) of zero meaning that they can only be removed from the DNS cache table by use of the **no ip localhost** *hostname ip-address* command. For the other entries shown, the timeout value is set with the **ip dns-ttl** command.

Related Commands

clear ip localhosts
ip dns-ttl
ip localhost

DHCP Commands

This chapter describes the commands used to configure Dynamic Host Configuration Protocol (DHCP) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure DHCP features, and configuration examples, see the "Configuring DHCP" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug dhcp

debug dhcp {**packet** | **preserve-state** | **all**}

no debug dhcp

Purpose

Enables the logging of Dynamic Host Configuration Protocol (DHCP) debug messages.

Command Mode

administrator exec

Syntax Description

packet	Specifies the debugging of packets that are processed by AOS.
preserve-state	Specifies that events relating to preserve-state are logged.
all	Specifies that both packet and preserve-state debugging are activated.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug dhcp** command to enable the logging of DHCP relay debug messages.

Caution Debugging can severely affect system performance. Caution should be exercised before enabling any debugging on a production system.

Use the **no** form of this command to disable DHCP debugging.

Examples

The following example enables debugging for DHCP packets:

```
[local]RedBack#debug dhcp packet
```

The following example enables debugging for secured-ARP entries:

```
[local]RedBack#debug dhcp preserve-state
```

The following sample log entries display when debugging for secured-ARP entries is enabled:

```
16:30:42 17Sep1999: %DHCP-7-PS_ENAB: DHCP Secured-ARP preserve state
enabled
16:37:04 17Sep1999: %DHCP-7-PS_ADD: Adding DHCP preserve-state
secured-ARP entry (host 10.0.154.100)
16:37:15 17Sep1999: %DHCP-7-PS_DISAB: DHCP Secured-ARP preserve state
disabled
```

Related Commands

dhcp relay option
dhcp relay size
show debugging

dhcp max-addrs

dhcp max-addrs *max-number*

no dhcp max-addrs

Purpose

Specifies the maximum number of Dynamic Host Configuration Protocol (DHCP) addresses to be assigned to a subscriber.

Command Mode

subscriber configuration

Syntax Description

max-number	Maximum number of unique IP addresses expected to be assigned by the DHCP server to hosts associated with a given subscriber circuit. The range of values is 1 to 255.

Default

None

Usage Guidelines

Use the **dhcp max-addrs** command within a subscriber record to indicate that associated hosts will use DHCP to dynamically acquire address information.

This command is helpful for load balancing the use of addresses from multiple pools. It is not enforced as a strict limit. Strict limits cannot be imposed by a DHCP relay; they can only be applied by the DHCP server.

Use the **no** form of this command to remove a maximum limit of DHCP addresses from a subscriber.

Examples

The following example configures the subscriber named `dhcp-test` to expect a total of eight IP addresses that can be allocated at any time:

```
[local]RedBack(config-ctx)#subscriber name dhcp-test
[local]RedBack(config-sub)#dhcp max-addrs 8
```

Related Commands

dhcp relay server
dhcp relay size

dhcp preserve-state

dhcp preserve-state

no dhcp preserve-state

Purpose

Instructs the Subscriber Management System (SMS) device to store Dynamic Host Configuration Protocol (DHCP) state information to nonvolatile storage.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **dhcp preserve-state** command to instruct the SMS device to store DHCP state information to non-volatile storage. A PCMCIA SRAM card must be in the system and formatted appropriately (using the **format** command) before it can carry out the DHCP preserve-state function.

Once the card is formatted and the **dhcp preserve-state** command has been executed, then DHCP can store information on SRAM regarding DHCP-added secured Address Resolution Protocol (ARP) entries. This information allows the secured-ARP and authentication, authorization and accounting (AAA) information to be recovered when a system reloads or when an I/O module is replaced (for I/O modules that support module extract). The information included for each entry is the context, the circuit handle, and the IP address.

Use the **no** form of this command to remove the instruction to the SMS device to use the SRAM for nonvolatile storage of DHCP state information.

Examples

The following example first formats the PCMCIA SRAM card for DHCP nonvolatile storage and then instructs the SMS device to store the DHCP state information to that nonvolatile storage:

```
[local]RedBack#format /pcmcia0 dhcp-secured-arp
[local]RedBack#config
[local]RedBack(config)#dhcp preserve-state
```

Related Commands

format

dhcp relay option

dhcp relay option

no dhcp relay option

Purpose

Enables the sending of Dynamic Host Configuration Protocol (DHCP) options in all DHCP packets that are relayed by the Subscriber Management System (SMS) device.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

DHCP relay options are not enabled.

Usage Guidelines

Use the **dhcp relay option** command to enable the sending of DHCP options in all DHCP packets that are relayed by the SMS. On some networks, DHCP is used to dynamically configure IP address information for subscriber hosts. The SMS device can act as a relay for DHCP servers. DHCP is typically used with RFC 1483- or RFC 1490-encapsulated circuits, and not Point-to-Point (PPP) circuits.

When this feature is enabled, the Access Operating System (AOS) adds relay options to all DHCP requests that are forwarded by the SMS on behalf of a DHCP client. DHCP relay options are described in the Internet Draft, *DHCP Relay Agent Information Option*, draft-ietf-dhc-agent-options-12.txt.

The AOS can use DHCP relay options to help track DHCP requests. Some options can also enhance the DHCP server's function. For example, an **agent remote id** option contains the ASCII username associated with the circuit and the DHCP server can use this circuit to make address allocation decisions. For AOS tracking purposes, the **agent circuit id** option contains a 32-bit number that identifies the circuit through which a subscriber has connected.

In order for relay options to take effect, DHCP relay must be enabled for the context using the **dhcp relay server** command and for an interface using the **dhcp relay size** command in interface configuration mode. Use the **dhcp max-addrs** command within a subscriber record to indicate that associated hosts are to use DHCP relay to dynamically acquire address information.

Use the **no** form of this command to disable the sending of DHCP relay options by the SMS device.

Examples

The following example enables DHCP relay options:

```
[local]RedBack(config-ctx)#dhcp relay option
```

Related Commands

dhcp relay server
dhcp relay size

dhcp relay server

dhcp relay server *ip-address*

no dhcp relay server *ip-address*

Purpose

Enables the relay of Dynamic Host Configuration Protocol (DHCP) messages and configures the IP address of a DHCP server.

Command Mode

context configuration

Syntax Description

ip-address	IP address of a target DHCP server.

Default

The relay of DHCP packets by the Subscriber Management System (SMS) device is disabled.

Usage Guidelines

Use the **dhcp relay server** command to enable the relay of DHCP messages and configure the IP address of a DHCP server. To enable communications with more than one server (with a limit per context of five), you can enter the **dhcp relay server** command multiple times.

In addition to enabling DHCP relay for the context using the **dhcp relay server** command, you must enable one or more interfaces using the **dhcp relay size** command in interface configuration mode. Use the **dhcp max-addrs** command within a subscriber record to indicate that associated hosts are to use DHCP relay to dynamically acquire address information.

Use the **no** form of this command to remove the corresponding server from the list of configured DHCP servers. Removing all servers disables the relaying of DHCP packets by the SMS device.

Examples

The following example enables DHCP relay and establishes that all packets are to be relayed to the DHCP server at IP address `10.1.1.1`:

```
[local]RedBack(config-ctx)#dhcp relay server 10.1.1.1
```

Related Commands

dhcp max-addrs
dhcp relay option
dhcp relay size

dhcp relay size

dhcp relay size *max-number*

{**no** | **default**} **dhcp relay size** *max-number*

Purpose

Enables Dynamic Host Configuration Protocol (DHCP) relay through the corresponding interface and specifies the maximum number of IP addresses to be assigned to the subnet connected to that interface.

Command Mode

interface configuration

Syntax Description

max-number	Maximum number of unique IP addresses to be assigned by the DHCP server for hosts on the same subnet as the configured interface. The range of values is 0 to 65,535; the default value is 0.

Default

The DHCP relay size is set to 0; DHCP relay is disabled.

Usage Guidelines

Use the **dhcp relay size** command to make an interface eligible for the relay of DHCP packets. In other words, the Subscriber Management System (SMS) device does not relay DHCP messages received on an interface, unless this command is present in the configuration for that interface. The SMS device uses this value for load balancing the use of addresses from multiple pools. It is not enforced as a strict limit. Strict limits cannot be imposed by a DHCP relay; they can only be applied by the DHCP server.

Use the **no** or **default** form of this command to remove the setting of the maximum number of IP addresses from the specified interface. Setting the *max-number* argument to 0 has the same effect.

Examples

The following example configures the interface named `dhcp-test` with an IP address of `10.1.1.1 255.255.255.0`. It is subsequently configured to indicate a total of `253` IP addresses that can be allocated by the DHCP server at any time from the `10.1.1.0` subnet:

```
[local]RedBack(config-ctx)#interface dhcp-test
[local]RedBack(config-if)#ip address 10.1.1.1 255.255.255.0
[local]RedBack(config-if)#dhcp relay size 253
```

Related Commands

dhcp max-addrs
dhcp relay server

dhcp server default-lease-time

dhcp server default-lease-time *seconds*

default dhcp server default-lease-time

Purpose

Determines the length of time an IP address is leased by the internal Dynamic Host Configuration Protocol (DHCP) server when an explicit lease time is not requested.

Command Mode

interface configuration

Syntax Description

seconds	Number of seconds that the IP address is leased.

Default

The default lease time is 86,400 seconds (one day).

Usage Guidelines

Use the **dhcp server default-lease-time** command to determine the length of time an IP address is leased by the internal DHCP server.

Common lease times are 86,400 seconds (one day), 604,800 seconds (one week), and 2,592,000 seconds (30 days).

Use the **default** form of this command to return the lease time to the default of one day.

Examples

The following example leases the IP address `10.1.1.1` for one week (`604800` seconds):

```
[local]RedBack(config-if)#dhcp server default-lease-time 604800
```

Related Commands

dhcp server max-lease-time
dhcp server range

dhcp server filename

dhcp server filename *filename*

no dhcp server filename *filename*

Purpose

For a device connected to the Subscriber Management System (SMS) device, configures the device's boot file via the Dynamic Host Configuration Protocol (DHCP) server.

Command Mode

interface configuration

Syntax Description

filename	Name of the system boot file.

Usage Guidelines

Use the **dhcp server filename** command to configure a device's boot file via the DHCP server.

Use the **no** form of this command to disable configuring a device's boot file via the DHCP server.

Examples

The following example configures a device's boot file called `sysboot` via the DHCP server:

```
[local]RedBack(config-if)#dhcp server filename sysboot
```

Related Commands

dhcp server range

dhcp server max-lease-time

dhcp server max-lease-time *seconds*

default dhcp server max-lease-time

Purpose

Determines the maximum length of time an IP address is leased by the internal Dynamic Host Configuration Protocol (DHCP) server.

Command Mode

interface configuration

Syntax Description

seconds	Maximum amount of time, in seconds, that an IP address is leased by the DHCP server. The range of values is 1 to 31,536,000.

Default

None

Usage Guidelines

Use the **dhcp server max-lease-time** command to determine the maximum length of time an IP address is leased by the internal DHCP server.

Examples

In the following example, the maximum length of time an IP address is leased is `600` seconds:

```
[local]RedBack(config-if)#dhcp server max-lease-time 600
```

Related Commands

dhcp server default-lease-time
dhcp server range
show dhcp server lease

dhcp server next-server

dhcp server next-server *ip-address*

no dhcp server next-server *ip-address*

Purpose

Configures a secondary Dynamic Host Configuration Protocol (DHCP) server to load share with the primary DHCP server, or to act as a backup to the primary DHCP server.

Command Mode

interface configuration

Syntax Description

ip-address	IP address of the secondary DHCP server.

Default

None

Usage Guidelines

Use the **dhcp server next-server** command to configure a secondary DHCP server to load share with the primary DHCP server, or to act as a backup to the primary DHCP server.

Use the **no** form of this command to remove a secondary DHCP server from the configuration.

Examples

The following example configures a secondary DHCP server at IP address `10.10.2.2`:

```
[local]RedBack(config-if)#dhcp server next-server 10.10.2.2.2
```

Related Commands

dhcp server range

dhcp server option

dhcp server option *option*

no dhcp server option *option*

Purpose

Configures Dynamic Host Configuration Protocol (DHCP) server options.

Command Mode

interface configuration

Syntax Description

option	Option to be configured. Table 29-1 in the "Usage Guidelines" section lists the standard UNIX options. Options are described in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*.

Default

None

Usage Guidelines

Use the **dhcp server option** command to configure DHCP server options.

Options are described in detail in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*. Table 29-1 lists all options. This section describes a few of the commonly used options.

Use the **domain-name-server** *ip-address* construct to specify a Domain Name System (DNS) server available to the client. In the registration context, the IP address of this interface is provided in response to DNS requests.

Use the **log-server** *ip-address* construct to specify a MIT-LCS UDP log server available to the client. You *must* configure this option before an interface can support cable modems.

Use the **router** *ip-address* construct to specify the IP address of the router on the client's subnet. The DHCP server uses the address of the interface that corresponds to the IP address.

Use the **subnet-mask** *ip-address* construct to specify the client's subnet mask. If no subnet mask option is provided, the DHCP server uses the subnet mask for the network on which an IP address is being assigned.

Use the **time-offset** *value* construct to specify, in seconds, the offset of the client's subnet from Coordinated Universal Time (UTC). If no value is set, the DHCP server uses 0 as the time offset.

Use the **time-server** *ip-address* construct to specify the time server that is available to the client. If no value is set, the DHCP server uses the IP address of the interface that corresponds to the assigned IP address.

Table 29-1 dhcp server option Command Options

• **1...255** {**numeric *value*** {**1** | **2** | **4**} | **string** *string*}	• **nisplus-server**
• **all-subnets-local** *value*	• **nntp-server**
• **arp-cache-timeout** *value*	• **non-local0-source-routing**
• **bootfile-name** *filename*	• **ntp-servers**
• **broadcast** *ip-address*	• **path-mtu-aging-timeout** *value*
• **cookie-server** *ip-address*	• **path-mtu-plateau-table** *value*
• **default-ip-ttl** *value*	• **perform-mask-discovery** *value*
• **default-tcp-ttl** *value*	• **policy-filter** *ip-address netmask*
• **domain-name** *string*	• **pop-server** *ip-address*
• **domain-name-server** *ip-address*	• **resource-location-server** *ip-address*
• **extensions-path** *string*	• **root-path** *string*
• **finger-server** *ip-address*	• **router** *ip-address*
• **font-server** *ip-address*	• **router-discovery** *value*
• **host-name** *ip-address*	• **router-solicitation-address** *ip-address*
• **ieee802-3-encapsulation** *value*	• **smtp-server** *ip-address*
• **ien116-name-server** *ip-address*	• **static-route** *ip-address netmask*
• **impress-server** *ip-address*	• **streettalk-directory-assistance-server** *ip-address*
• **interface-mtu** *value*	• **streettalk-server** *ip-address*
• **ip-fowarding** *value*	• **subnet-mask** *ip-address*
• **irc-server** *ip-address*	• **swap-server** *ip-address*
• **log-server** *ip-address*	• **tcp-keepalive-garbage** *value*
• **lpr-server** *ip-address*	• **tcp-keepalive-interval** *value*
• **mask-supplier** *value*	• **tftp-server-name** *string*
• **max-dgram-reassembly** *value*	• **time-offset** *value*
• **merit-dump** *string*	• **time-server** *ip-address*
• **mobile-ip-home-agent** *ip-address*	• **trailer-encapsulation** *value*
• **netbios-dd-server *ip-address***	• **vendor-encapsulated-options** {**numeric** *value* {**1** | **2** | **4**} | **string** *string*}
• **netbios-name-server *ip-address***	• **www-server** *ip-address*
• **netbios-scope** *string*	• **x-display-manager** *ip-address*
• **nis-domain** *string*	

Examples

The following example configures the DNS server at IP address `10.10.1.1`:

```
[local]RedBack(config-if)#dhcp-server option domain-name-server 10.1.1.1
```

Related Commands

dhcp relay server

dhcp server range

dhcp server range {**all** | *ip-address ip-address*}

no dhcp server range {**all** | *ip-address ip-address*}

Purpose

Enables the internal Dynamic Host Configuration Protocol (DHCP) server to assign IP addresses.

Command Mode

interface configuration

Syntax Description

all	Specifies that all IP addresses in the subnet defined by the interface can be assigned by the DHCP server, with the exception of the interface's IP address.
ip-address	Explicit range of IP addresses that can be assigned by the DHCP server.

Default

None

Usage Guidelines

Use the **dhcp server range** command to enable the internal DHCP server to assign IP addresses.

Use the **no** form of this command to disable the ability to assign IP addresses.

Examples

The following example enables the DHCP server to assign all IP addresses, except for that of the interface:

```
[local]RedBack(config-if)#dhcp server range all
```

Related Commands

dhcp server default-lease-time
dhcp server filename
dhcp server max-lease-time
dhcp server next-server
dhcp server option

format

format *device* [**dhcp-secured-arp**]

Purpose

Reformats a device and completely deletes its contents.

Command Mode

administrator exec

Syntax Description

device	Name of the device to be formatted.
dhcp-secured-arp	Optional. Specifies that the device is to be formatted for use as Dynamic Host Configuration Protocol (DHCP) nonvolatile storage. Valid only for PCMCIA SRAM cards.

Default

None

Usage Guidelines

Use the **format** command to reformat a device and completely delete its contents. The possible devices are **/flash**, **/pcmcia0**, and **/pcmcia1**. Only the last two devices can be used with the **dhcp-secured-arp** keyword.

Caution This command completely erases all contents of the specified device. Think carefully before reformatting the device that contains the system image and configuration files.

Note This command description also appears in Chapter 4, “System Image and Configuration File Commands.”

Examples

The following example erases the `/flash` device and reformats it for future use:

```
[local]RedBack#format /flash
```

The following example shows the messages you see when you use the **format** command on a device that is already formatted:

```
[local]RedBack#format /pcmcia0 dhcp-secured-arp

Device /pcmcia0 contains a file system.
Proceed with format of /pcmcia0? [confirm]
```

If you press **Enter** to confirm, the system reformats the device as you have specified.

If the device already contains DHCP-secured Address Resolution Protocol (ARP) formatting, the messages look like the following example:

```
[local]RedBack#format /pcmcia0

Device /pcmcia0 is formatted for dhcp-secured-arp.
Proceed with format of /pcmcia0? [confirm]
```

Related Commands

directory
mkdir
rmdir

show dhcp

show dhcp {**interface** [*if-name*] | **preserve-state** [**pre-bind** [**all**] | **secured-arp** [**all**]]}

Purpose

Displays Dynamic Host Configuration Protocol (DHCP) information by an interface or as related to the DHCP preserve state.

Command Mode

operator exec

Syntax Description

interface	When used without the optional *if-name* argument, specifies that you want to display information for all interfaces in the current context.
if-name	Optional. Specific interface about which you want information displayed.
preserve-state	Specifies that you want preserve state information displayed.
pre-bind	Optional if the **preserve-state** keyword is used. Specifies that you want information about SRAM entries awaiting binding to be displayed.
secured-arp	Optional if the **preserve-state** keyword is used. Specifies that you want to display information about SRAM secured Address Resolution Protocol (ARP) entries.
all	Optional if either the **pre-bind** or **secured-arp** keyword is used. Specifies that entries for all contexts are to be displayed.

Default

None

Usage Guidelines

Use the **show dhcp** command to display DHCP information by interface or as related to the DHCP preserve state. When used with the **interface** keyword, the display includes the number of addresses that have been assigned by DHCP to the interface and the DHCP relay server size for the interface. When used with the **preserve-state** keyword, the display includes the status of the DHCP preserve state and if enabled, the counters for the SRAM contents.

Additional detailed information is included if you specify the **pre-bind** or **secured-arp** keywords. The **all** keyword expands the display to include the secured-ARP or pre-bind entries for all contexts.

Examples

The following example provides sample output for the **show dhcp** command when no keywords are used and the DHCP preserve state is enabled:

```
[local]RedBack>show dhcp preserve-state

DHCP Preserve State is ON
SRAM device /pcmcia0 contains:
0 context names
0 entries used by context names
0 IO module information entries
0 secured-ARP entries
0 entries awaiting binding
0 entries marked as deleted
0 total entries used
314567 free entries
```

The following example shows the display if a secured-ARP entry exists:

```
[local]RedBack>show dhcp preserve-state

DHCP Preserve State is ON
SRAM device /pcmcia0 contains:
1 context names
2 entries used by context names
1 IO module information entries
1 secured-ARP entries
0 entries awaiting binding
0 entries marked as deleted
4 total entries used
314563 free entries
```

The following example shows the display when DHCP preserve state is disabled:

```
[local]RedBack>show dhcp preserve-state

DHCP Preserve State is OFF
SRAM device /pcmcia0 available
```

The following example shows the command and the resulting display when used with the **secured-arp all** construct:

```
[local]RedBack>show dhcp preserve-state secured-arp all

Host         Circuit  Context
10.0.154.100 30000001 local
```

The following example shows the command and the resulting display when used with the **pre-bind all** construct:

```
[local]RedBack>show dhcp preserve-state pre-bind all

Host         Circuit  Context
10.0.154.100 29000020 local
```

The following example shows the command and the resulting display when used with the **interface** keyword:

```
[local]RedBack>show dhcp interface all

        Total  Addrs   Addrs
Type    Addrs  In-Use  Avail  Interface
------  -----  ------  -----  ---------
Server    253       0    253  int1
Server    253       0    253  int2
Server    253       0    253  int3
```

Related Commands

dhcp preserve-state
format

show dhcp server lease

show dhcp server lease [**all** | **circuit** {*slot/port* {*vpi vci* | [*hdlc-channel*] *dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** [*cm-slot-*] *session-id*} | **interface** *if-name* | **ip** *ip-address* | **mac** *mac-address*]

Purpose

Displays information on IP address leases provided by the internal Dynamic Host Configuration Protocol (DHCP) server.

Command Mode

operator exec

Syntax Description

all	Optional. Displays leases for all contexts.
circuit	Optional. Displays leases for the specified circuit.
slot/port	Slot number followed by a slash (/) and the port number. Used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay ports. The range of slot values is 0 to 31. The range of port values is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI). Used with ATM ports. The range of *vpi* argument values is 0 to 255. For ATM T1 modules, the range of *vci* argument values is 1 to 1,023; for ATM DS-3 Version 1 modules, the range of *vci* argument values is 1 to 2,047; for ATM OC-3 Version 1 modules, the range of *vci* argument values is 1 to 4,095; for all ATM Version 2 modules, the range of *vci* argument values is 1 to 65,535.
hdlc-channel	Optional when you include the *dlci* argument. Name of the HDLC channel in the case for a channelized DS-3 port. This argument is required for channelized DS-3 modules and not allowed in any other case.
dlci	Data-link connection identifier (DLCI). Used with Frame Relay ports. The range of values is 16 to 991.
lac *vcn*	Optional. Layer 2 Tunneling Protocol Access Controllers (LAC) virtual circuit number (VCN). The range of values is 0 to 65,534.
lns *vcn*	Optional. Layer 2 Tunneling Protocol Network Services (LNS) virtual circuit number (VCN). The range of values is 0 to 65,534.
pppoe [*cm-slot-*] *session-id*	Optional. Point-to-Point Protocol over Ethernet (PPPoE) specification. The *cm-slot* argument is required for Connection Manager (CM) modules and not used in any other case. It specifies the CM slot number. The session ID must be entered for all product platforms. The range of *session-id* argument values is 1 to 65,534.

interface *if-name*	Optional. Name of the interface for which you want to display lease information.
ip *ip-address*	Optional. IP address for which you want to display lease information.
mac *mac-address*	Optional. Media access control (MAC) address for which you want to display lease information.

Default

None

Usage Guidelines

Use the **show dhcp server lease** command to display information on IP address leases provided by the internal DHCP server.

Examples

The following example provides sample output from the **show dhcp server lease** command:

```
[local]RedBack>show dhcp server lease all

MAC-Address         IP-Address   Mins-Rem   Cct-Handle   Interface@Context
00:90:27:2d:c8:64   10.0.154.2   0          0x31000001   i1@local
```

Related Commands

dhcp server max-lease-time
dhcp server range

show dhcp server sram

show dhcp server sram

Purpose

Displays information on the Dynamic Host Configuration Protocol (DHCP) server synchronous RAM (SRAM).

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show dhcp server sram** command to display information on the DHCP server SRAM.

Examples

The following example provides sample output from the **show dhcp server sram** command:

```
[local]RedBack>show dhcp server sram

 0 context names
 0 entries used by context names
 0 IO module information entries
 0 lease entries
 0 total entries used
24572 free entries
```

Related Commands

dhcp server range

Chapter 30

NTP Commands

This chapter describes the commands used to configure and maintain Network Time Protocol (NTP) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure NTP, and configuration examples, see the "Configuring NTP" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug ntp

debug ntp {**all** | **packets** | **update**}

no debug ntp

Purpose

Enables debugging of the Network Time Protocol (NTP) feature.

Command Mode

administrator exec

Syntax

all	Displays all NTP debugging messages.
packets	Displays only messages on incoming and outgoing NTP packets.
update	Displays only messages on NTP update packets.

Default

NTP debugging is disabled.

Usage Guidelines

Use the **debug ntp** command to enable NTP debugging.

Caution Debugging can severely affect system performance. Exercise caution when enabling any debugging on a production system.

Use the **no** form of this command to disable debugging of NTP.

Examples

The following command enables debugging of NTP:

```
[local]RedBack#debug ntp
```

Related Commands

logging console
ntp server
show ntp associations
show ntp status
terminal monitor

ntp mode

ntp mode

Purpose

Enters Network Time Protocol (NTP) configuration mode where NTP parameters can be set.

Command Mode

global configuration

Syntax

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **ntp mode** command to enter NTP configuration mode. Use the commands in NTP configuration mode to set NTP parameters.

Examples

The following example changes the mode from global configuration to NTP configuration:

```
[local]RedBack(config)#ntp mode
[local]RedBack(config-ntp)#
```

Related Commands

None

ntp server

ntp server *ip-address* [**context** *ctx-name*] [**prefer**] [**source** *if-name*] [**version** *ver-num*]

no ntp server *ip-address*

Purpose

Starts the Network Time Protocol (NTP) daemon and synchronizes the Subscriber Management System (SMS) device time with a remote NTP server.

Command Mode

global configuration

Syntax Description

ip-address	IP address of the remote NTP server.
context *ctx-name*	Optional. Context in which the destination address is reachable. Use this construct when the NTP server must be reached through a context other than local.
prefer	Optional. Marks the NTP server as the preferred server when multiple NTP servers are configured.
source *if-name*	Optional. SMS device interface that is to be used for NTP traffic.
version *ver-num*	Optional. NTP version used. The version options are 1, 2, and 3; the default is 3.

Default

The context for the NTP server is the local context. The NTP version is 3.

Usage Guidelines

Use the **ntp server** command to enable the SMS device clock to synchronize with an external clock source. A remote NTP client cannot synchronize with the SMS device.

Use the **context** *ctx-name* construct to specify a server that is reachable through a context other than the local context. Use the **prefer** keyword to mark an NTP server as the preferred server to use when multiple NTP servers are configured. Use the **source** *if-name* construct to choose the SMS device interface that is to be used for NTP traffic. Use the **version** *ver-num* construct to change the NTP version from the default of 3.

Use the **no** form of this command to disable NTP services on the SMS device.

Examples

The following example configures the SMS NTP client to synchronize with an NTP remote server at IP address `10.1.1.1`. The server is also marked as the preferred server:

```
[local]RedBack(config)#ntp server 10.1.1.1 prefer
```

Related Commands

debug ntp
show ntp associations
show ntp status

show ntp associations

show ntp associations

Purpose

Displays current associations with Network Time Protocol (NTP) remote servers and lists NTP daemon statistics for those servers.

Command Mode

operator exec

Syntax

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show ntp associations** command to display current associations with NTP remote servers and list NTP daemon statistics for those servers.

Examples

The following example shows that synchronization has taken place:

```
[local]RedBack>show ntp associations

remote           local    st  poll reach delay    offset     disp
=10.1.1.2        0.0.0.0  4   64   377   0.99944  -0.003611  0.0.1596
=155.53.200.100  0.0.0.0  3   64   377   0.99939  -0.003486  0.01598
```

Estimates based on network delay (delay), dispersion of time packet exchanges (disp), clock offset (offset), and the IP address of the remote NTP server are displayed.

The following example shows that the NTP daemon has been started, but is currently trying to synchronize with the remote server:

```
[local]RedBack>show ntp associations

remote          local      st  poll reach  delay    offset     disp
=10.1.1.2       10.1.1.1   16  64   0      0.00000  0.000000   16.0000
```

If the daemon has not been started, no output is provided under the list of headings.

Related Commands

debug ntp
show ntp status

show ntp status

show ntp status

Purpose

Displays current internal Network Time Protocol (NTP) parameter settings and synchronization status.

Command Mode

operator exec

Syntax

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show ntp status** command to display the current internal NTP parameter settings and synchronization status. If the default behavior is not modified; that is, if the **slowsync** command has not been enabled, it takes a few minutes for the NTP daemon to adjust time with valid NTP servers. While the NTP daemon is in the process of collecting samples from remote NTP servers, the “Synch source not available yet” message is displayed.

Examples

The following example shows that synchronization has taken place:

```
[local]RedBack>show ntp status

Ntpd version 3-5.93e
system peer:      155.53.200.100
system peer mode: server
leap indicator:   00
stratum:          3
precision:        -18
root distance:     0.28976 s
root dispersion:   0.07988 s
reference time:    bb7fceda.55994000  Tue, Sep 7 1999  17:50:18.334
system flags:      bclient monitor
frequency:         0.000 ppm
stability:         32.834 ppm
```

The following example shows that the NTP daemon has been started, but is currently trying to synchronize with the remote server:

```
[local]RedBack>show ntp status

Ntpd version 3-5.93e
Synch source not available yet
```

The following example shows the output when the daemon has not been started:

```
[local]RedBack>show ntp status

Ntpd version 3-5.93e
... not running
```

Related Commands

debug ntp
show ntp associations
slowsync

slowsync

slowsync

no slowsync

Purpose

Configures the Subscriber Management System (SMS) device to slowly adjust its local clock rate to compensate for differences with a remote clock source.

Command Mode

NTP configuration

Syntax

This command has no keywords or arguments.

Default

Gradual adjustment of the local clock rate is disabled.

Usage Guidelines

Use the **slowsync** command to change the rate of the SMS device clock so that it gradually converges with the NTP server clock—provided the initial difference in time between the two clocks is less than 16 minutes. If the time difference is more than 16 minutes, synchronization does not occur.

The NTP daemon adjusts the SMS device clock within a few minutes, if the difference between the SMS device clock and the remote NTP server is greater than five seconds (and less than 16 minutes). This adjustment occurs within the first five minutes after the NTP daemon is started.

Use the **no** form of this command to disable gradual adjustment of the local clock rate.

Examples

The following example enables gradual adjustment of the local clock rate:

```
[local]RedBack(config-ntp)#slowsync
```

Related Commands

show ntp status

Part 9

Routing

Basic IP Routing Commands

This chapter describes the commands used to configure and maintain basic IP routing features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure basic IP routing, and configuration examples, see the "Configuring Basic IP Routing" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug ip irdp

debug ip irdp [**circuit** {*slot/port* {*vpi vci* | *hdlc-channel dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*}]

no debug ip irdp [**circuit** {*slot/port* {*vpi vci* | *hdlc-channel dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*}]

Purpose

Enables the logging of Internet Control Message Protocol (ICMP) Router Discovery Protocol (IRDP) debug messages.

Command Mode

administrator exec

Syntax Description

circuit	Optional. Limits the logging of IRDP debug messages to the specified circuit.
slot/port	Slot and port. Used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay I/O modules. The range of values for the *slot* argument is 0 to 31. The range of values for the *port* argument is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI). Used with ATM ports. The range of values for the *vpi* argument is 0 to 255. The range of values for the *vci* argument depends on the I/O module: • ATM T1—1 to 1,023 • ATM DS-3 (version 1)—1 to 2,047 • ATM OC-3 (version 1)—1 to 4,095 • ATM (version 2)—1 to 65,535
hdlc-channel	Name of the High-Level Data Link Control (HDLC) channel on the channelized DS-3 port. This argument is required for channelized DS-3 modules and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) used with Frame Relay ports. The range of values is 16 to 991.
lac *vcn*	Layer 2 Tunneling Protocol Access Controllers (LAC) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.
lns *vcn*	Layer 2 Tunneling Protocol Network Services (LNS) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.

pppoe *cm-slot-session-id* Point-to-Point Protocol over Ethernet (PPPoE) session. The *cm-slot* argument is required for Connection Manager (CM) modules on the SMS 10000 device and is not used in any other case. It specifies the CM slot number. The *session-id* argument must be specified for all product platforms; the range of values is 1 to 65,534.

Default

Disabled

Usage Guidelines

Use the **debug ip irdp** command to enable the logging of IRDP debug messages.

When debugging is enabled, all messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables debug logging for IRDP:

```
[local]RedBack#debug ip irdp
```

Related Commands

logging console
terminal monitor

debug ip route

debug ip route

no debug ip route

Purpose

Enables the logging of debug messages related to configuring, modifying, and deleting IP routes.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Usage Guidelines

Use the **debug ip route** command to enable the logging of debug messages related to IP route changes, including route additions, changes, or deletions. Use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables the logging of debug messages related to adding IP routes:

```
[local]RedBack#debug ip route

18:15:00 19Jun2001: CE: %GTD-7-AR: Adding to the RIB a route for interface far-east:
200.3.2.20/255.255.255.0
18:15:00 19Jun2001: CE: %GTD-7-IFCG: routing: interface 200.1.6.9 (south) event Add
18:15:00 19Jun2001: CE: %GTD-7-AR: Adding to the RIB a route for interface south:
200.1.6.9/255.255.255.0
```

```
18:15:00 19Jun2001: CE: %GTD-7-IFCG: routing: interface 200.1.9.12 (west) event Add
18:15:00 19Jun2001: CE: %GTD-7-AR: 3Adding to the RIB a route for interface west:
200.1.9.12/255.255.255.0
```

Related Commands

ip route
logging console
router bgp
router ospf
router rip
show ip route
terminal monitor

debug ip routing

debug ip routing

no debug ip routing

Purpose

Enables the logging of debug messages related to IP routing processes.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Usage Guidelines

Use the **debug ip routing** command to enable the logging of debug messages related to IP routing processes. Use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables the logging of debug messages for routing processes:

```
[local]RedBack#debug ip routing

18:16:31 19Jun2001: CE: %IP-7-STRT_DEL: Deleting static route to 0.0.0.0/0.0.0.0
18:16:31 19Jun2001: CE: %IP-7-RT_DEL: Deleting route to 0.0.0.0/0.0.0.0
18:16:31 19Jun2001: CE: %IP-7-XFER_RT_DEL: TX to FE: opcode: route del, addr
0.0.0.0/0.0.0.0
```

Related Commands

ip route
logging console
router bgp
router ospf
router rip
show ip route
terminal monitor

ip irdp

ip irdp [**broadcast**] [**lifetime** *value*] [**maximum** *value*] [**minimum** *value*] [**preference** *value*]

no ip irdp [**broadcast**] [**lifetime** *value*] [**maximum** *value*] [**minimum** *value*] [**preference** *value*]

Purpose

Enables the Internet Control Message Protocol (ICMP) Router Discovery Protocol (IRDP) on the interface.

Command Mode

interface configuration

Syntax Description

broadcast	Optional. Causes advertisements to be sent using the broadcast address 255.255.255.255.
lifetime *value*	Optional. Length of time, in seconds, a host retains and uses information in an IRDP advertisement. Advertisements should arrive well before the lifetime expiration of prior advertisements. The range of values is 4 to 9,000. The default value is 3 times the maximum interval.
maximum *value*	Optional. Maximum amount of time, in seconds, between IRDP advertisements. The range of values is 4 to 1,800. The default value is 600.
minimum *value*	Optional. Minimum amount of time, in seconds, between IRDP advertisements. The range of values is 3 to 1,800. The default value is 0.75 times the maximum advertisement interval. This value cannot be larger than the maximum advertisement interval.
preference *value*	Optional. Degree of preference. The range of values is 0x0 to 0xffffffff.

Default

Disabled

Usage Guidelines

Use the **ip irdp** command to enable hosts to learn their default route via router-transmitted advertisement packets instead of through manual configuration of the hosts. IRDP sends advertisements on a regular basis and also in response to host solicitations, which are typically generated when a host boots up.

When a host has multiple routers directly connected to it, each of the routers can send IRDP advertisements to the host. The host will select the advertised route with with the highest preference. The 0x80000000 special value indicates that the advertised route should not be used by hosts as the default router IP address. If an interface is configured with secondary addresses, all addresses are advertised with the same preference.

Examples

The following example enables the interface named `customers` at IP address `10.1.1.1 255.255.255.0` to use IRDP to advertise the default route to hosts:

```
[local]RedBack(config-ctx)#interface customers
[local]RedBack(config-if)#ip address 10.1.1.1 255.255.255.0
[local]RedBack(config-if)#ip irdp maximum 1800 minimum 1700 lifetime 9000
```

Related Commands

debug ip irdp
show ip interface

ip maximum-paths

ip maximum-paths *maximum*

default ip maximum-paths

Purpose

Enables equal-cost multipath forwarding to a particular destination.

Command Mode

context configuration

Syntax Description

maximum	Number of equal-cost paths applied to the routing table for a particular destination. The range of values is 1 to 6. The default value is 1.

Default

The default value is 1; equal-cost multipath routing is disabled.

Usage Guidelines

Use the **ip maximum-paths** command to enable equal-cost multipath forwarding or to change the currently configured number of maximum paths to a destination.

Equal-cost multipath forwarding uses a hash threshold algorithm to spread session traffic equally among as many as six paths to a destination. The algorithm selects a path based on the source and destination addresses and the source and destination ports. Once the algorithm decides on a path, packets between a given source and destination are forwarded along that path. The path is altered only if network topology changes. This mechanism reduces the chance of out-of-order packet delivery for a specific flow.

Open Shortest Path First (OSPF) and static IP routing support equal-cost multipath forwarding.

Use the **default** form of this command to disable equal-cost multipath forwarding.

Examples

The following example sets the maximum number of paths in the routing table to 5:

```
[local]RedBack(config-ctx)#ip maximum-paths 5
```

Related Commands

ip route

ip route

ip route {*ip-address netmask ip-address if-name*} [**precedence** *value*] [**cost** *value*]

no ip route {*ip-address netmask ip-address if-name*} [**precedence** *value*] [**cost** *value*]

Purpose

Configures one or more static IP routes.

Command Mode

context configuration
subscriber configuration

Syntax Description

ip-address	IP address of the target network or subnet.
netmask	Network mask where the 1 bits indicates the network, or subnet, and the 0 bits indicate the host portion of the network address provided.
ip-address	IP address of a next-hop router that can reach the target network or subnet.
if-name	Name of the outgoing interface to use for the target network or subnet.
precedence *value*	Optional. Route preference when compared against all other routes. A lower value indicates a more-preferred route. The range of values is 10 to 225.
cost *value*	Optional. Route preference when compared against other static routes. A lower value indicates a more-preferred route. The range of values is 0 to 15.

Default

If no precedence is specified, the static route is assumed to have a precedence of 10. If no cost is specified, the static route is assumed to have a cost of 0.

Usage Guidelines

Use the **ip route** command to configure one or more static IP routes. Once configured, a static route stays in the routing database indefinitely. When multiple static routes are configured for a single destination and the outbound interface of the current static route goes down, a backup route is activated. Up to six static routes can be configured for a single destination.

Each static route can be configured with a precedence value, a cost value, or both. When configuring routes and support for multiple protocols, ensure that the precedence values for each route type are distinct from one another. For example, ensure that the precedence value for BGP routes is distinct from static IP routes, which are also distinct from the precedence value configured for OSPF routes.

Among multiple routes with the same destination, the preferred route is selected in the following order:

1. The route with the lowest precedence value is preferred first.
2. If there are two or more routes with the same precedence value, the route with the lowest cost value is preferred.
3. If there are two or more routes with the same precedence and cost values, the route with the lowest IP address is preferred.
4. When redistributing static routes, routing protocols ignore the cost value assigned to those static routes. If static routes are redistributed through dynamic routing protocols, only active static routes to a destination is advertised.

Table 31-1 lists the default precedence values for routes learned through various protocols.

Table 31-1 Protocol Precedence Defaults

Protocol	Precedence Value
Directly connected	0
Static IP	10
Subscriber record	15
OSPF—internal to the autonomous system	60
RIP	100
OSPF—external to the autonomous system	150
BGP	170

When equal-cost multipath forwarding is enabled, the system selects a subset of routes to install in the forwarding table. The maximum number of routes installed depends on the current maximum path configuration. For example, if you set the number of maximum paths to 2 using the **ip maximum-paths** command, and you configure three static routes of equal cost and precedence to the same destination, only two of these routes are submitted to the route table manager as best path candidates. The third is held in reserve as a floating route.

To configure a default static IP route, use 0.0.0.0 for the network number and mask. A valid next-hop address and interface is required.

Use the **no** form of this command to delete a static route from the routing database.

Examples

The following example routes packets for network `10.10.0.0/16` via interface `enet1` to the device at IP address `10.3.2.1`:

```
[local]RedBack(config-ctx)#ip route 10.10.0.0 255.255.0.0 10.3.2.1 enet1
```

The following example, with an IP default route with a cost of `2`, uses `atm5` as the outgoing interface and the device at IP address `10.1.1.1` as the next-hop router:

```
[local]RedBack(config-ctx)#ip route 0.0.0.0 0.0.0.0 10.1.1.1 atm5 2
```

In the following example, the first static route, `atm5` has a default cost of 0, and therefore, will be used as the active route. Both `eth6` and `atm6` have the same cost (2). In the event that `atm5` goes down, `atm6` becomes the interface with the preferred route, because its IP address is lower than that of `eth6`.

```
[local]RedBack(config-ctx)#ip route 0.0.0.0 0.0.0.0 10.1.1.1 atm5
[local]RedBack(config-ctx)#ip route 0.0.0.0 0.0.0.0 172.21.200.254 eth6 2
[local]RedBack(config-ctx)#ip route 0.0.0.0 0.0.0.0 10.1.1.1 atm6 2
```

The following example configures two equal-cost routes to the same destination `1.0.0.0`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip maximum-paths 2
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 3.3.3.3 nhop3 cost 5
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 4.4.4.4 nhop4 cost 5
```

The following example displays the two routes configured in the previous example:

```
[local]RedBack#show ip route

Destination       Nexthop     Protocol    Precedence   Cost   Ttl
1.0.0.0/8         3.3.3.3     static      10           5      infinity
                  4.4.4.4     static      10           5      infinity
```

The following example configures an additional route to the same destination `1.0.0.0`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 2.2.2.2 nhop2 cost 5
```

The following example displays the routing table, which has been updated with the addition of the route configured in the previous example. Because the next-hop IP address of 2.2.2.2 and 3.3.3.3 are lower than the 4.4.4.4 IP address, and because the maximum paths to the destination is set to 2, the 4.4.4.4 next-hop IP address is removed from the routing table.

```
[local]RedBack#show ip route

Destination      Nexthop       Protocol     Precedence   Cost  Ttl
1.0.0.0/8        2.2.2.2       static       10           5     infinity
                 3.3.3.3       static       10           5     infinity
```

The following example configures a new route that supersedes all the previously configured routes because it has a lower cost (0 versus 5):

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 5.5.5.5 nhop5
```

The following example displays the updated routing table. Previously configured routes are held in floating status in case this route becomes unavailable.

```
[local]RedBack#show ip route

Destination      Nexthop       Protocol     Precedence   Cost  Ttl
1.0.0.0/8        5.5.5.5       static       10           0     infinity
```

Related Commands

debug ip route
ip route—subscriber configuration mode
precedence—BGP configuration, BGP group configuration, and BGP peer configuration modes
precedence—OSPF configuration mode
precedence—RIP configuration mode
preference
show ip route
show ip static-route

show ip route

show ip route [*ip-address* [*netmask*] | **detail**]

Purpose

Displays IP route information.

Command Mode

operator exec

Syntax Description

ip-address	Optional. Destination IP address of the route to be displayed.
netmask	Optional. Network mask.
detail	Optional. Adds protocol-specific metric information to the output display.

Default

Displays all IP routes in the current context.

Usage Guidelines

Use the **show ip route** command without any arguments or keywords to display the entire routing table used for IP data forwarding in the current context. If an IP address is specified without a mask, the best match (longest-prefix match) route used for data forwarding to that destination is displayed.

Examples

The following example displays **show ip route detail** command output. Table 31-2 describes the fields.

```
[local]RedBack>show ip route detail

Status codes: * valid, > best
  Network         Nexthop         Metric  Precedence    Protocol
*>10.1.1.0/24     10.1.1.1        0       0             direct
*>20.1.1.0/24     20.1.1.1        0       0             direct
*>30.0.0.0/8      20.1.1.5        0       170           bgp
*                 10.1.1.2        1       200           rip
*>35.0.0.0/8      10.1.1.2        1       200           rip
*>40.0.0.0/8      20.1.1.5        0       170           bgp
*                 10.1.1.2        1       200           rip
*>50.0.0.0/8      20.1.1.5        0       170           bgp
```

```
*                 10.1.1.2        1       200           rip
*>80.0.0.0/8      10.1.1.9        0       65            static
*>90.0.0.0/8      20.1.1.9        0       65            static
*>110.0.0.0/8     blackhole       0       130           aggregate
*>110.2.0.0/16    10.1.1.9        0       65            static
*>110.3.0.0/16    10.1.1.9        0       65            static
*>145.0.0.0/8     155.53.145.232  0       65            static
*>155.53.0.0/16   155.53.145.254  0       65            static
*>155.53.145.0/24 155.53.145.231  0       0             direct
```

Table 31-2 show ip route detail Field Descriptions

Field	Description
Network	Destination prefix and the prefix length
Nexthop	IP address of the next system that is used when forwarding a packet to the destination
Metric	Protocol-specific cost of the route
Precedence	Precedence of the route
Protocol	Protocol from which the route was learned

The following example displays **show ip route** output. Table 31-3 describes the fields.

```
[local]RedBack>show ip route

Destination       Nexthop        Protocol    Prec   Cost   Ttl
10.1.1.0/24       enet0          direct      0      0      infinity
20.1.1.0/24       enet1          direct      0      0      infinity
30.0.0.0/8        20.1.1.5       bgp         170    0      infinity
35.0.0.0/8        10.1.1.2       rip         200    1      160
40.0.0.0/8        20.1.1.5       bgp         170    0      infinity
50.0.0.0/8        20.1.1.5       bgp         170    0      infinity
110.0.0.0/8       blackhole      aggregate   130    0      infinity
110.2.0.0/16      10.1.1.9       static      65     0      infinity
110.3.0.0/16      10.1.1.9       static      65     0      infinity
155.53.145.0/24   mgmt           direct      0      0      infinity
```

The following example configures two equal-cost routes to the same destination `1.0.0.0`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 3.3.3.3 nhop3
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 4.4.4.4 nhop4
```

The following example displays the two routes configured in the previous example:

```
[local]RedBack>show ip route

Destination       Nexthop     Protocol    Precedence   Cost   Ttl
1.0.0.0/8         3.3.3.3     static      10           0      infinity
                  4.4.4.4     static      10           0      infinity
```

The following example configures an additional route to the same destination `1.0.0.0`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#ip route 1.0.0.0 255.0.0.0 2.2.2.2 nhop2
```

The following example displays the routing table, which has been updated with the addition of the route configured in the previous example. Because the next-hop IP addresses of `2.2.2.2` and `3.3.3.3` are lower than the 4.4.4.4 IP address, and because the maximum paths to the destination is set to 2, the 4.4.4.4 next-hop IP address is removed from the routing table.

```
[local]RedBack>show ip route

Destination      Nexthop       Protocol     Precedence   Cost  Ttl
1.0.0.0/8        2.2.2.2       static       10           0     infinity
                 3.3.3.3       static       10           0     infinity
```

The following example displays **show ip route** *ip-address* output. Table 31-3 describes the fields.

```
[local]RedBack>show ip route 35.0.0.0

Destination       Nexthop         Protocol    Prec     Cost     Ttl
35.0.0.0/8        10.1.1.2        rip         200      1        165
```

Table 31-3 show ip route *prefix* Field Descriptions

Field	Description
Destination	Destination prefix and the prefix length
Nexthop	IP address of the next system that is used when forwarding a packet to the destination
Protocol	Protocol from which the route was learned
Prec	Precedence of the route
Cost	Protocol-specific cost of the route
Ttl	Time-to-live for the route

Related Commands

debug ip route
ip route
precedence—BGP configuration, BGP group configuration, and BGP peer configuration modes
precedence—OSPF configuration mode
precedence—RIP configuration mode
preference
router bgp
router ospf
router rip

show ip static-route

show ip static-route [*ip-address* [*netmask*]]

Purpose

Displays static routing table entries in the current context.

Command Mode

operator exec

Syntax Description

ip-address	Optional. Destination IP address of static route to display.
netmask	Optional. Network mask.

Default

Displays all statically configured routes in the current context.

Usage Guidelines

Use the **show ip static-route** without any arguments to display all statically configured routing table entries for IP data forwarding in the current context. The *ip-address* argument specifies the network or subnet address of the destination. The *netmask* argument specifies the network mask associated with that address. If an address is specified without the mask, the best route (longest-prefix match) for data forwarding to that destination is displayed.

Examples

The following example displays statically configured IP routes:

```
[local]RedBack>show ip static-route

Destination         Nexthop         Protocol      Cost   Ttl
0.0.0.0/0           eth00           static        0      infinity
```

The following example indicates the preferred route (*) among three static IP routes to the same destination.

```
[local]RedBack>show ip static-route

Destination         Nexthop         Protocol      Cost   Ttl
*0.0.0.0/0          atm5            static        0      infinity
0.0.0.0/0           atm6            static        2      infinity
0.0.0.0/0           eth6            static        2      infinity
```

Related Commands

ip route
show ip route

Chapter 32

RIP Commands

This chapter describes the commands used to configure and maintain Routing Information Protocol (RIP) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure RIP, and configuration examples, see the "Configuring RIP" chapter in the *Access Operating System (AOS) Configuration Guide*.

auto-summary

auto-summary

{**no** | **default**} **auto-summary**

Purpose

Enables automatic network number summarization (autosummarization) for Routing Information Protocol version 2 (RIPv2).

Command Mode

RIP configuration

Syntax Description

This command has no keywords or arguments.

Default

Autosummarization is enabled when the **network** command is enabled.

Usage Guidelines

Use the **auto-summary** command to enable autosummarization for RIPv2. This command enables the Access Operating System (AOS) to summarize subprefixes to Class A, Class B, and Class C network boundaries when class network boundaries are crossed.

Use the **no** and **default** forms of this command to disable autosummarization.

Examples

The following example disables autosummarization in RIPv2:

```
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#no auto-summary
```

Related Commands

network
show ip route
version

debug ip rip

debug ip rip

no debug ip rip

Purpose

Enables the logging of Routing Information Protocol (RIP) debug messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip rip** command to enable the logging of RIP debug messages. Use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable RIP debugging.

Examples

The following example enables the logging of RIP debug messages:

```
[local]RedBack#debug ip rip

10:42:23 11Feb2000: %IP-7-RIP_TX_UPD: RIP: sending v1 update to 255.255.255.255 via a
(10.1.1.254) len 24
10:42:23 11Feb2000: %IP-7-RIP1_RT2: network 11.0.0.0, metric 0
```

Related Commands

ip rip listen
ip rip receive version
ip rip send version
ip rip split-horizon
ip rip supply
network
logging console
show ip route
terminal monitor
version

ip rip interface-cost

ip rip interface-cost *cost*

{**no** | **default**} **ip rip interface-cost**

Purpose

Configures the routing cost associated with the Routing Information Protocol (RIP) interface.

Command Mode

interface configuration

Syntax Description

cost	Interface cost. The range of values is 1 to 15. The default cost is null, or 0.

Default

The default cost assigned to an interface is 0.

Usage Guidelines

Use the **ip rip interface-cost** command to configure the routing cost associated with the RIP interface. The cost value is used as a metric for route selection. The lower the cost, the more likely an interface is to be used to forward data traffic.

This command does not apply to loopback interfaces.

Use the **no** or **default** form of this command to return the cost to the default value of 0.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Examples

The following example assigns a cost of `5` to the interface `atm1`:

```
[local]RedBack(config-ctx)#interface atm1
[local]RedBack(config-if)#ip rip interface-cost 5
```

Related Commands

show ip interface

ip rip listen

ip rip listen

no rip listen

Purpose

Enables an interface to receive Routing Information Protocol (RIP) packets.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

Any interface whose IP address is part of the network, specified by the **network** command in RIP configuration mode, can receive RIP packets.

Usage Guidelines

Use the **ip rip listen** command to enable an interface to receive RIP packets.

This command does not apply to loopback interfaces.

Use the **no** form of this command to return the interface to its default behavior.

Example

The following example enables the interface `enet1` to receive RIP packets:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip rip listen
```

Related Commands

ip rip supply
network
show ip interface

ip rip receive version

ip rip receive version {**1** | **2**}

no ip rip receive version {**1** | **2**}

Purpose

Restricts the interface to receive only the specified version of Routing Information Protocol (RIP) packets.

Command Mode

interface configuration

Syntax Description

1	Accepts only RIP version 1 packets.
2	Accepts only RIP version 2 packets.

Default

The RIP version of an incoming packet that is accepted by an interface is determined by the **version** command in RIP configuration mode.

Usage Guidelines

Use the **ip rip receive version** command to restrict the interface to receive only the specified version of RIP packets. All other interfaces continue to receive the version specified by the **version** RIP configuration mode command.

This command does not apply to loopback interfaces.

Use the **no** form of this command to return the RIP version to its default value.

Examples

The following example restricts the interface `enet1` to receive only RIP version 2 packets:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip rip receive version 2
```

Related Commands

ip rip send version
show ip interface
version

ip rip send version

ip rip send version {**1** | **2**}

no ip rip send version {**1** | **2**}

Purpose

Restricts the interface to send only the specified version of Routing Information Protocol (RIP) packets.

Command Mode

interface configuration

Syntax Description

1	Sends only RIP version 1 packets.
2	Sends only RIP version 2 packets.

Default

The RIP version of packets sent by an interface is determined by the **version** command in RIP configuration mode.

Usage Guidelines

Use the **ip rip send version** command to restrict the specified interface to send only the specified version of RIP packets. All other interfaces continue to send the version specified by the **version** RIP configuration mode command.

This command does not apply to loopback interfaces.

Use the **no** form of this command to return the version to its default value.

Examples

The following example restricts the interface `enet1` to send only RIP version 2 packets:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip rip send version 2
```

Related Commands

ip rip receive version
show ip interface
version

ip rip split-horizon

ip rip split-horizon

no ip rip split-horizon

Purpose

Enables Routing Information Protocol (RIP) split-horizon processing on an interface.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

Split-horizon processing is enabled.

Usage Guidelines

Use the **ip rip split-horizon** command to enable split-horizon processing on an interface. Split-horizon processing prevents routing loops in distance-vector routing protocols, such as RIP. It blocks route information from being advertised out any interface from which the information originated. The split-horizon mechanism is intended to speed up convergence after a link failure.

This command does not apply to loopback interfaces.

Use the **no** form of this command to disable split-horizon processing on an interface.

Examples

The following example disables split horizon processing on an interface named `enet1`:

```
[local]RedBack(config-ctx)#int enet1
[local]RedBack(config-if)#no ip rip split-horizon
```

Related Commands

show ip interface

ip rip supply

ip rip supply

no ip rip supply

Purpose

Enables the specified interface to send Routing Information Protocol (RIP) packets.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

Any interface whose IP address is part of the network specified by the **network** command in RIP configuration mode is enabled to send RIP packets.

Usage Guidelines

Use the **ip rip supply** command to enable the specified interface to send RIP packets. If more than one circuit is bound to an interface, the interface does not send RIP packets out any of those circuits.

This command does not apply to loopback interfaces.

The **no** form of this command is used to prevent the interface from sending RIP packets.

Examples

The following example enables the sending of RIP packets on the interface `enet1`:

```
[local]RedBack(config-ctx)#interface enet1
[local]RedBack(config-if)#ip rip supply
```

Related Commands

ip rip listen
network
show ip interface

network

network *network*

no network *network*

Purpose

Specifies a network for which directly connected interfaces automatically receive and send Routing Information Protocol (RIP) updates.

Command Mode

RIP configuration

Syntax Description

network	IP Class A, Class B, or Class C network number or the network number of an interface in the current context.

Default

None

Usage Guidelines

Use the **network** command to specify a network for which directly connected interfaces automatically receive and send RIP updates. You can specify multiple **network** commands. Any interface whose IP address has the same network prefix as the *network* argument is automatically enabled to send and receive RIP updates. Use this command in conjunction with the **router rip** command in context configuration mode.

To disable RIP for specific interfaces within a network that sends and receives RIP packets, use the **no ip rip send** and **no ip rip listen** interface configuration mode commands.

Use the **no** form of this command to remove the specified network.

Examples

The following example configures RIP to be used on all interfaces directly connected to the `10.0.0.0` network:

```
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#network 10.0.0.0
```

Related Commands

router rip
show ip route

precedence

precedence *precedence*

no precedence

Purpose

Configures the precedence for routes learned from the Routing Information Protocol (RIP) routing process.

Command Mode

RIP configuration

Syntax Description

precedence	Precedence of the route. The range of values is 10 to 255. The default value is 100. A lower value indicates a more-preferred route.

Default

Routes learned from RIP have a precedence of 100.

Usage Guidelines

Use the **precedence** command to set the precedence for routes learned from RIP. A lower value indicates a more-preferred route. The Access Operating System (AOS) assigns a default value to each routing protocol process. Table 32-1 lists the default values.

Table 32-1 Protocol Precedence Defaults

Protocol	Precedence Value
Directly connected	0
Static IP	10
Subscriber record	15
OSPF—internal to the autonomous system	60
RIP	100
OSPF—external to the autonomous system	150
Border Gateway Protocol (BGP)	170

When configuring routes for multiple protocols, ensure that the *precedence* argument for each route type is distinct from the other. For example, ensure that the *precedence* argument for Border Gateway Protocol (BGP) routes is distinct from static IP routes, which must also be distinct from Open Shortest Path First (OSPF) routes, and so on.

Use the **no** form of this command to return the *precedence* argument to the default value of 100.

Examples

The following example sets the RIP precedence to `180`:

```
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#precedence 180
```

Related Commands

ip route—context configuration mode
precedence—BGP configuration mode, BGP group configuration mode, BGP peer configuration mode
precedence—OSPF configuration mode
show ip route

redistribute

redistribute {**bgp** | **direct** | **ospf** | **static** | **subscriber**} [**metric** *metric*]

no redistribute {**bgp** | **direct** | **ospf** | **static** | **subscriber**} [**metric** *metric*]

Purpose

Redistributes routes learned through protocols other than the Routing Information Protocol (RIP) into the RIP routing process.

Command Mode

RIP configuration

Syntax Description

bgp	Redistributes all Border Gateway Protocol (BGP) routes present in the context into the RIP routing process.
direct	Redistributes directly attached networks defined in interface profiles into the RIP routing process.
ospf	Redistributes all Open Shortest Path First (OSPF) routes present in the context into the RIP routing process.
static	Redistributes all routes statically configured in the context into the RIP routing process.
subscriber	Redistributes routes configured within subscriber records into the RIP routing process.
metric *metric*	Optional. Metric used for the redistributed route. The range of values is 0 to 16. The default value is 0.

Default

Only directly attached networks are redistributed into the RIP domain. The default metric value is 0.

Usage Guidelines

Use the **redistribute** command to redistribute routes learned through protocols other than RIP into the RIP routing process. You can use this command multiple times to configure several redistribution patterns.

Use the **no** form of this command to disable routes learned through non-RIP protocols from being redistributed into the RIP routing process.

Examples

The following example redistributes all configured static IP routes into the RIP routing process:

```
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#redistribute static
```

The following example prevents all directly attached networks from being redistributed into the RIP routing process:

```
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#no redistribute direct
```

The following example redistributes all BGP routes into the RIP routing process with a metric of 1:

```
[local]RedBack(config-rip)#redistribute bgp metric 1
```

Related Commands

ip route
router bgp
router ospf
router rip
show ip route

router rip

router rip

no router rip

Purpose

Enables the Routing Information Protocol (RIP) routing process and enters RIP configuration mode.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

RIP is disabled.

Usage Guidelines

Use the **router rip** command to enable the RIP routing process and enter RIP configuration mode. Use this command in conjunction with the **network** command in RIP configuration mode.

Use the **no** form of this command to disable the RIP routing process.

Examples

The following example enables the RIP routing process in the local context:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#
```

Related Commands

auto-summary
network

version

version {**1** | **2**}

no version

Purpose

Specifies the Routing Information Protocol (RIP) version for the current context.

Command Mode

RIP configuration

Syntax Description

1	Specifies RIP version 1.
2	Specifies RIP version 2.

Default

The Access Operating System (AOS) receives RIP version 1 and 2 packets, but sends only version 1 packets.

Usage Guidelines

User the **version** command to configure the RIP version for the current context. The RIP version can be modified on explicit interfaces through the **ip rip receive version** and **ip rip send version** commands in interface configuration mode.

Use the **no** form of this command to restore the default behavior.

Examples

The following example configures RIPv2 for the local context:

```
[local]RedBack(config-ctx)#router rip
[local]RedBack(config-rip)#version 2
```

Related Commands

ip rip receive version
ip rip send version
show ip route

OSPF Commands

This chapter describes the commands used to configure and maintain Open Shortest Path First (OSPF) protocol features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure OSPF, and configuration examples, see the “Configuring OSPF” chapter in the *Access Operating System (AOS) Configuration Guide*.

area

area {*id* | *ip-address*}

no area {*id* | *ip-address*}

Purpose

Configures an Open Shortest Path First (OSPF) area and enters OSPF area configuration mode.

Command Mode

OSPF configuration

Syntax Description

id	32-bit number. The range of values is 0 to 4,294,967,295. 0 is reserved for the backbone area.
ip-address	IP address. The 0.0.0.0 address is reserved for the backbone area.

Default

None

Usage Guidelines

Use the **area** command to configure an OSPF area. Multiple areas are supported. Specify the area identifier or IP address for the SMS device to use when participating in OSPF routing. All SMS devices in an area must use the same area identifier to establish adjacencies, or neighbors. To specify that the SMS device is directly connected to the OSPF backbone, use the command and argument **area** *0.0.0.0* or **area** *0.*

Use the **no** form of this command to remove the OSPF area.

Examples

The following example configures an area using an address of `34.0.0.0`:

```
[local]RedBack(config-ospf)#area 34.0.0.0
[local]RedBack(config-ospf-area)#
```

Related Commands

area-sumrange
areatype
show ip ospf area
show ip ospf border-router

area-sumrange

area-sumrange *ip-address netmask* [**not-advertise**]

no area-sumrange *ip-address netmask* [**not-advertise**]

Purpose

Summarizes inter-area routes advertised by an Open Shortest Path First (OSPF) area border router (ABR).

Command Mode

OSPF area configuration

Syntax Description

ip-address	IP address of the route.
netmask	Network mask of the IP address specified.
not-advertise	Optional. Prevents the specified route from being advertised in interarea route summarizations.

Default

Route address ranges for interarea route summarization are not specified.

Usage Guidelines

Use the **area-sumrange** command to carry out inter-area route summarization. This command is only relevant when the Subscriber Management System (SMS) device is configured as an ABR. Use the **not-advertise** keyword to prevent the specified route from being advertised in route summarizations.

Use the **no** form of this command to disable route summarization for a particular summary range. All individual routes contained in the summary range are advertised to other areas.

Examples

The following example displays the routes that fall into the range `10.1.0.0 255.255.0.0` that will be advertised in interarea route summaries:

```
[local]RedBack(config-ospf-area)#area-sumrange 10.1.0.0 255.255.0.0
```

Related Commands

area
areatype
show ip ospf summary-range

areatype

areatype {**nssa** [**always translate** | **noredistribute** | **nosummary**] | **stub** [**nosummary**]}

{**no** | **default**} **areatype**

Purpose

Defines an Open Shortest Path First (OSPF) area as a stub area or as a not-so-stubby-area (NSSA).

Command Mode

OSPF area configuration

Syntax Description

nssa	Configures the area as an NSSA.
always translate	Optional. Configures the Access Operating System (AOS) to always translate Type 7 NSSA-external link-state advertisements (LSAs) to Type 5 AS-external LSAs. If these keywords are not specified, the NSSA area border router (ABR) with the highest route ID performs the translation. These keywords are useful when the Subscriber Management System (SMS) device is configured as ABR.
noredistribute	Optional. Configures the AOS to not redistribute Type 7 NSSA-external LSAs into NSSAs. This keyword is useful when the SMS device is configured as an ABR located between an external-capable area and an NSSA. This keyword ensures that routes redistributed via the **redistribute** command in OSPF configuration mode are injected only into normal areas, not into NSSAs.
nosummary	Optional. Instructs the AOS not to advertise Type 3 summary LSAs into the stub area or NSSA. This option can be used with the **nssa** or **stub** keyword. This option only has impact when the SMS device is configured as an ABR.
stub	Configures the area as a stub type.

Default

The area type is normal.

Usage Guidelines

Use the **areatype nssa** construct to configure an NSSA. NSSAs are an extension of OSPF stub areas. Their intent is to preserve the properties of a stub area, but also allow limited import of external routes from other routing domains. These routes are imported as Type 7 NSSA-external LSAs, which are flooded only within the NSSA. For propagation of these routes to other areas, Type 7 LSAs must be translated into type 5 external LSAs by NSSA ABRS. Use the **noredistribute** keyword when you want the redistribute command to import routes only into normal areas, not into NSSAs.

Use the **areatype stub** construct to configure a stub area. Type 5 AS-external-LSAs and Type 4 summary-LSAs are not flooded into a stub area, thereby reducing the link-state database size and the processor and memory usage of routers inside stub areas. Instead, a stub area relies on default routing to forward traffic addressed to external destinations. You must configure all routers in a stub area as stub area routers. You cannot configure the backbone as a stub area.

Use the **no** or **default** form of this command to return the specified area to a normal area.

Examples

The following example configures area 4 as a stub area:

```
[local]RedBack(config-ospf)#area 4
[local]RedBack(config-ospf-area)#areatype stub
```

The following example configures area 5 as an NSSA:

```
[local]RedBack(config-ospf)#area 5
[local]RedBack(config-ospf-area)#areatype nssa
```

Related Commands

defaultroute
nssa-sumrange
show ip ospf area

as-sumrange

as-sumrange *ip-address netmask* [**not-advertise**]

no as-sumrange *ip-address netmask* [**not-advertise**]

Purpose

Summarizes inter-autonomous system routes redistributed into an Open Shortest Path First (OSPF) domain by an autonomous system boundary router (ASBR).

Command Mode

OSPF configuration

Syntax Description

ip-address	Network address of the route.
netmask	Network mask of the specified IP address.
not-advertise	Optional. Suppresses the sending of Type 5 link-state advertisements (LSAs) for routes contained in the specified IP address range.

Default

Route address ranges for interautonomous system summarization are not specified.

Usage Guidelines

Use the **as-sumrange** command to summarize interautonomous system routes that are redistributed into an OSPF domain. This command is only relevant when the Subscriber Management System (SMS) device is configured as an ASBR. The SMS device redistributes information about routes that are external to the autonomous system into the OSPF domain via Type 5 external-LSAs. Because information about the external routes is summarized, the size of the OSPF routing table is reduced.

Use the **not-advertise** keyword to block routes that are contained in the summary range from being redistributed into the OSPF domain.

Use the **no** form of this command to disable route summarization of an IP address block and allow all individual routes to be redistributed into OSPF domains.

Examples

The following example configures RIP routes that fall into the `10.0.0.0 255.0.0.0` range to be summarized and redistributed into OSPF:

```
[local]RedBack(config-ospf)#as-sumrange 10.0.0.0 255.0.0.0
```

Related Commands

redistribute—OSPF configuration mode
show ip ospf summary-range

authentication

authentication {**simple** *password* | **md5 keyid** *keyid password*}

{**no** | **default**} **authentication** {**simple** *password* | **md5 keyid** *keyid password*}

Purpose

Enables authentication and specifies the authentication scheme for the Open Shortest Path First (OSPF) interface.

Command Mode

OSPF interface configuration

Syntax Description

simple *password*	Simple authentication password. The *password* argument is an alphanumeric string of 1 to 8 characters.
md5 keyid *keyid password*	MD5 authentication key ID. The range of values for the *keyid* argument is 0 to 4,294,967,295. The *password* argument is an alphanumeric string of 1 to 16 characters.

Default

Authentication is not enabled.

Usage Guidelines

Use the **authentication** command to enable authentication and specify the authentication scheme for the OSPF interface. All routers connected to the same IP subnet must use the same authentication scheme and password.

When MD5 authentication is enabled, every OSPF packet carries an MD5 digest that is generated by the originating router and checked by the receiving router. When a router receives an OSPF packet on an interface, it must authenticate the MD5 checksum. Packets that fail MD5 authentication are discarded.

If multiple MD5 key IDs have been configured, all configured key IDs are sent out for authentication until all neighbors are using the most recently-configured key ID or until the other key IDs are removed from the configuration.

Use the **no** or **default** form of this command to disable authentication. To disable MD5 authentication, the keyid must be specified and all configured keyids must be removed.

Examples

The following example configures simple authentication with a password of `secret`:

```
[local]RedBack(config-ospf-interface)#authentication simple secret
```

The following example configures MD5 authentication, using a key ID of `1` and the password `test`:

```
[local]RedBack(config-ospf-interface)#authentication md5 keyid 1 test
```

Related Commands

ospf-interface
show ip ospf interface

cost

cost *cost*

{**no** | **default**} **cost**

Purpose

Specifies the cost of sending a packet out the Open Shortest Path First (OSPF) interface.

Command Mode

OSPF interface configuration

Syntax Description

cost	Cost of the OSPF interface. The range of values is 1 to 6,5535. The default value is 1.

Default

The cost is 1.

Usage Guidelines

Use the **cost** command to configure the cost of sending a packet out the OSPF interface. Only one cost can be assigned per interface. The **redistribute** command always redistributes external routes as Type 2.

Use the **no** or **default** form of this command to return the cost to its default value.

Examples

The following example sets an interface to a cost of 3:

```
[local]RedBack(config-ospf-interface)#cost 3
```

Related Commands

debug ip ospf
ospf-interface
redistribute—OSPF configuration mode
show ip ospf interface

debug ip ospf

debug ip ospf database | **packet** {**ack** | **all** | **dd** | **hello** | **lsr** | **lsu**}| **policy** | **spf** | **state**}

no debug ip ospf database | **packet** {**ack** | **all** | **dd** | **hello** | **lsr** | **lsu**}| **policy** | **spf** | **state**}

Purpose

Enables the logging of Open Shortest Path First (OSPF) debug messages.

Command Mode

administrator exec

Syntax Description

database	Enables database, adjacency, and flooding debugging.
packet	Enables the logging of debug messages for the specified packet type, described below.
ack	Enables the logging of debug messages for only OSPF acknowledgement packets.
all	Enables the logging of debug messages for all OSPF packets.
dd	Enables the logging of debug message for only OSPF database description packets.
hello	Enables the logging of debug messages for only OSPF Hello packets.
lsr	Enables the logging of debug messages for only OSPF link-state request packets.
lsu	Enables the logging of debug messages for only OSPF link-state update packets.
policy	Enables the logging of debug messages for OSPF redistribution policies.
spf	Enables the logging of debug messages for shortest path first (SPF) computations.
state	Enables the logging of debug messages for OSPF events and state transitions.

Default

None

Usage Guidelines

Use the **debug ip ospf** command to enable the logging of OSPF debug messages. Use the **logging console** and **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable logging of OSPF debug messages.

Examples

The following example enables debug logging messages for OSPF Hello packets:

```
[local]RedBack#debug ip ospf packet hello
```

Related Commands

logging console
show ip ospf
terminal monitor

default-originate

default-originate [**always**] [**metric** *metric*]

no default-originate

Purpose

Configures an autonomous system boundary router (ASBR) to originate a default route into the Open Shortest Path First (OSPF) domain.

Command Mode

OSPF configuration

Syntax Description

always	Optional. Specifies that the system originates the default route into the OSPF domain regardless of whether or not there is an active default route available for redistribution by the ASBR.
metric *metric*	Optional. Metric value for the default route. The range of values is 0 to 16,777,215. The default value is 1. The metric type is always specified as a Type 2 external route metric.

Default

An ASBR does not originate default routes into the OSPF domain.

Usage Guidelines

Use the **default-originate** command to configure an ASBR to originate a default route into the OSPF domain. This command is intended for use in Type 5 external link-state advertisement-capable areas.

If you enter this command without any keywords, the system originates the default route into the OSPF domain, only if there is an active default route for redistribution. For example, if you are redistributing only static routes into OSPF, a default route is originated only if there is an active static default route in the routing table. Use the **always** keyword to inject the default route into the OSPF domain, regardless of whether or not there is an active default route available.

Use the **metric** *metric* construct to configure a preference for the default route. A lower metric value indicates a preferred route. If there are two routers injecting a default route with the same value, the router closest to the Subscriber Management System (SMS) device is selected.

Examples

The following example configures the system to always originate a default route with a metric of `10`:

```
[local]RedBack(config-ospf)#default-originate always metric 10
```

Related Commands

redistribute
show ip ospf

defaultroute

defaultroute [**metric** *metric*]

no defaultroute [**metric** *metric*]

Purpose

Enables a default route to be injected into an Open Shortest Path First (OSPF) stub area or not-so-stubby-area (NSSA).

Command Mode

OSPF area configuration

Syntax Description

metric *metric*	Optional. Metric value for the default route. The range of values is 1 to 1,677,215. The default value is 1.

Default

No default route is propagated into a stub area or NSSA.

Usage Guidelines

Use the **defaultroute** command to inject a route into a stub area or NSSA. The default route in stub areas is always a Type 3 route and is only injected into the stub area if the Subscriber Management System (SMS) device is an area border router (ABR).

Default routing in NSSAs has different implications, depending on the specific configuration. If this command is used with an NSSA ABR, a Type 7 default route if injected into the NSSA. If this command is used with an NSSA ABR that is configured with the **areatype nssa nosummary** command, a Type 3 default route is originated into the NSSA. If this command is used with an NSSA ASBR, Type 7 default routes are injected into the NSSA, if present in the external routing table.

Use the **metric** *value* construct to assign a preference for the default route. A lower metric value indicates a preferred route. If there are two routers injecting a default route with the same metric value, the router closest to the Subscriber Management System (SMS) device is selected.

Use the **no** form of this command to remove the default route.

Examples

The following example configures a default route metric value of 3:

```
[local]RedBack(config-ospf)#defaultroute metric 3
```

Related Commands

area
areatype
show ip ospf area

hello-interval

hello-interval *interval*

{**no** | **default**} **hello-interval**

Purpose

Configures the interval between Open Shortest Path First (OSPF) Hello packets sent out the interface.

Command Mode

OSPF interface configuration

Syntax Description

interval	Amount of time, in seconds, between Hello packets sent out the interface. The range of values is 1 to 255. The value must be the same for all nodes on a network. The default value is 10.

Default

The interval between Hello packets sent out an interface is 10 seconds.

Usage Guidelines

Use the **hello-interval** command to configure the interval between Hello packets sent out the interface. Routers send Hello packets at a fixed interval on all interfaces to establish and maintain neighbor relationships. This interval, which must be the same on all routers on a shared logical IP network, is advertised in the Hello interval field in the Hello packet. The smaller the Hello interval, the faster topological changes will be detected, but more routing traffic will ensue.

Use the **no** or **default** form of this command to return the interval value to its default setting.

Examples

The following example configures an interval between Hello packets to be 12 seconds:

```
[local]RedBack(config-ospf-interface)#hello-interval 12
```

Related Commands

ospf-interface
retransmit-interval
routerdead-interval
show ip ospf interface

nssa-sumrange

nssa-sumrange *prefix netmask* [**not-advertise**]

no nssa-sumrange *prefix netmask* [**not-advertise**]

Purpose

Controls the summarization of routes that are translated by an Open Shortest Path First (OSPF) not-so-stubby-area (NSSA) area border router (ABR).

Command Mode

OSPF area configuration

Syntax Description

prefix	Prefix of the route in the form A.B.C.D.
netmask	Prefix mask of the specified IP address.
not-advertise	Optional. Suppresses the translation of Type 7 link-state advertisements (LSAs) for routes contained in the specified IP address range.

Default

None

Usage Guidelines

Use the **nssa-sumrange** command to control the summarization of routes that are translated by an NSSA ABR. NSSA ABRs translate type 7 NSSA-external LSAs into Type 5 AS-external-LSAs when sending routes out of an NSSA to external-capable areas.

Use the **not-advertise** keyword to filter Type 7 LSAs in the summary range from being translated into Type 5 LSAs.

Use the **no** form of this command to disable route summarization of an IP address block and allow all individual routes in the range to be redistributed into OSPF domains.

Examples

The following example enables the translation of type 7 LSAs, originated from routes in the `10.0.0.0 255.0.0.0` range, into OSPF external-capable areas:

```
[local]RedBack(config-ospf-area)#nssa-sumrange 10.0.0.0 255.0.0.0
```

Related Commands

areatype
redistribute
show ip ospf summary-range

ospf-interface

ospf-interface *ip-address* {**broadcast** | **p2p** | **loopback**}

no ospf-interface *ip-address* {**broadcast** | **p2p** | **loopback**}

Purpose

Configures Open Shortest Path First (OSPF) routing on an existing interface for an area and enters OSPF interface configuration mode.

Command Mode

OSPF area configuration

Syntax Description

ip-address	IP address of the configured interface.
broadcast	Indicates that the interface is attached to a broadcast network.
p2p	Indicates that the interface is attached to a point-to-point (p2p) network.
loopback	Indicates that the interface has no association with any circuit. It is advertised as a host route with a cost of 0.

Default

None

Usage Guidelines

Use the **ospf-interface** command to enable an OSPF interface that connects to either:

- a broadcast network—broadcast networks support more than two attached routers and have the ability to address a single physical message to all attached routers.
- a point-to-point network—a point-to-point network joins a single pair of routers.
- a loopback interface—an interface that is not bound to any circuit.

OSPF routing must be enabled on at least one interface. That interface must already be configured for the context via the **interface** command in context configuration mode.

Caution Interfaces configured for OSPF can support only one circuit. If more than one circuit is configured for an OSPF interface, the OSPF interface placed in the DOWN state.

Caution If the interface IP address is changed using the **ip address** command in interface configuration mode, it affects the OSPF interface with which it is associated.

Use the **no** form of this command to disable OSPF routing on the specified interface.

Examples

The following example configures the interface at IP address `192.30.200.10` as a point-to-point link:

```
[local]RedBack(config-ospf-area)#ospf-interface 192.30.200.10 p2p
[local]RedBack(config-ospf-interface)#
```

Related Commands

interface
ip address
show ip ospf interface

precedence

precedence *internal external*

{**no** | **default**} **precedence**

Purpose

Sets the precedence for routes learned via the Open Shortest Path First (OSPF) protocol.

Command Mode

OSPF configuration

Syntax Description

internal	Value assigned to an OSPF route internal to the autonomous system. The range of values is 10 to 255. A lower value indicates a more-preferred route.
external	Value assigned to an OSPF route external to the OSPF system. The range of values is 10 to 255. A lower value indicates a more-preferred route.

Default

The precedence value for OSPF routes internal to the autonomous system is 60. The value for OSPF routes external to the autonomous system is 150.

Usage Guidelines

Use the **precedence** command to sets the precedence for routes learned via OSPF. A lower value indicates a more-preferred route. When configuring routes for multiple protocols, ensure that the *value* argument for each route type is distinct from the other. For example, ensure that the *value* argument for Border Gateway Protocol (BGP) routes is distinct from static IP routes, which must also be distinct from OSPF routes. The Access Operating System (AOS) assigns a default value to each routing protocol process.

Table 33-1 lists the default values.

Table 33-1 Protocol Precedence Defaults

Protocol	Precedence Value
Directly connected	0
Static IP	10
Subscriber record	15
OSPF—internal to the autonomous system	60
Routing Information Protocol (RIP)	100
OSPF—external to the autonomous system	150
Border Gateway Protocol (BGP)	170

Use the **no** or **default** form of this command to return the OSPF precedence value to its default precedence value of 60 or 150, depending on whether the routes are internal or external to the autonomous system.

Examples

The following example sets the OSPF precedence for internal routes to `80` and for external routes to `170`:

```
[local]RedBack(config-ospf)#precedence 80 170
```

Related Commands

debug ip ospf
default-originate
ip route
precedence—BGP configuration, BGP group configuration, and BGP peer configuration
precedence—RIP configuration mode
show ip ospf
spf-timers

redistribute

redistribute {**bgp** | **direct** | **rip** | **static** | **subscriber** [**metric** *metric*]}

no redistribute {**bgp** | **direct** | **rip** | **static** | **subscriber**}

Purpose

Redistributes routes learned through other protocols and methods into Open Shortest Path First (OSPF) networks.

Command Mode

OSPF configuration

Syntax Description

bgp	Redistributes routes learned through the Border Gateway Protocol (BGP) into the OSPF domain.
direct	Redistributes routes from directly attached networks into the OSPF domain.
rip	Redistributes routes from the Routing Information Protocol (RIP) process into the OSPF domain.
static	Redistributes static IP routes into OSPF.
subscriber	Injects routes configured within subscriber records.
metric *metric*	Optional. Cost of the redistributed routes. The range of values is 0 to 16,777,215. The default value is 20.

Default

Redistribution is not enabled.

Usage Guidelines

Use the **redistribute** command to redistribute routes learned through other protocols and methods into OSPF networks. More than one **redistribute** command can be specified.

Routes are redistributed using the Type 2 external route metric. Routes are redistributed as Type 5 AS-external LSAs in external-capable (normal) areas, and as Type 7 NSSA-external LSAs in NSSAs. This command does not enable the SMS device to redistribute a default route into the OSPF domain unless it is used in conjunction with the **default-originate** command in OSPF configuration mode.

Use the **no** form of this command to disable redistribution of the configured routing protocol into OSPF routing.

Examples

The following example redistributes routes learned through the RIP process into the OSPF domain:

```
[local]RedBack(config-ospf)#redistribute rip
```

Related Commands

debug ip ospf
default-originate
show ip ospf database

retransmit-interval

retransmit-interval *interval*

{**no** | **default**} **retransmit-interval**

Purpose

Configures the interval between Open Shortest Path First (OSPF) link-state advertisement (LSA) retransmissions by the interface.

Command Mode

OSPF interface configuration

Syntax Description

interval	Amount of time, in seconds, between LSA retransmissions sent out the interface. The range of values is 1 to 65,535. The default value is 5.

Default

The interval between LSA retransmissions sent out the interface is 5 seconds.

Usage Guidelines

Use the **retransmit-interval** command to configure the interval between LSA retransmissions sent out the interface. When a router sends LSAs to its neighbors, the router expects to receive an acknowledgment packet from the neighbor within a certain amount of time. If the router does not receive an acknowledgment, it retransmits the LSA.

Use the **no** or **default** form of this command to return the interval value to its default value.

Examples

The following example configures the retransmit interval to 7 seconds:

```
[local]RedBack(config-ospf-interface)#retransmit-interval 7
```

Related Commands

debug ip ospf
show ip ospf area
show ip ospf interface

routerdead-interval

routerdead-interval *interval*

{**no** | **default**} **routerdead-interval**

Purpose

Configures the amount of time the interface waits to receive an Open Shortest Path First (OSPF) Hello packet from a neighbor before determining that the neighbor is nonoperational.

Command Mode

OSPF interface configuration

Syntax Description

interval	Amount of time, in seconds, the interface waits to receive a Hello packet from a neighbor. The range of values is 1 to 65,535. The default value is 40. The value must be the same for all nodes on a common network.

Default

The interval the interface waits to receive a Hello packet from a neighbor is 40 seconds.

Usage Guidelines

Use the **routerdead-interval** command to configure the interval the interface waits to receive a Hello packet from a neighbor before determining that the neighbor is nonoperational. If a router does not receive a Hello packet from a neighbor in that interval, the router modifies its topological database to indicate that the neighbor is nonoperational. The router dead interval must be the same for all nodes on a common network, and must be greater than that of the Hello interval to avoid destroying adjacencies when the neighbor router is operational.

Use the **no** or **default** form of this command to return the router dead interval to its default value.

Examples

The following example configures the interval that the SMS will wait to receive a hello packet from its neighbor before determining the neighbor is nonoperational is 60 seconds:

```
[local]RedBack(config-ospf-interface)#routerdead-interval 60
```

Related Commands

debug ip ospf
hello-interval
show ip ospf interface

router-id

router-id *ip-address*

Purpose

Configures the Subscriber Management System (SMS) device identifier, which is exchanged in Open Shortest Path First (OSPF) routing messages.

Command Mode

context configuration

Syntax Description

ip-address	IP address of the interface that is used as the router identifier.

Default

A router ID is not preconfigured.

Usage Guidelines

Use the **router-id** command to identify the SMS device from which OSPF packets originated. You must first configure a router ID before the OSPF routing process can be enabled.

To modify or remove a router ID, disable the OSPF routing process.

Note This command is also described in the Chapter 34, “BGP Commands.”

Examples

The following example configures the IP address `192.34.200.10` as the router identifier:

```
[local]RedBack(config-ctx)#router-id 192.34.200.10
```

Related Commands

router bgp
router ospf
show ip ospf

router ospf

router ospf

no router ospf

Purpose

Enables Open Shortest Path First (OSPF) routing and enters OSPF configuration mode.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

OSPF routing is disabled.

Usage Guidelines

Use the **router ospf** command to enable OSPF routing in the current context. One OSPF routing process is supported per context. A router ID must be configured through the **router-id** command before the OSPF routing process can be enabled.

Use the **no** form of this command to disable OSPF routing.

Examples

The following example configures OSPF routing for the current context:

```
[local]RedBack(config-ctx)#router ospf
[local]RedBack(config-ospf)#
```

Related Commands

router-id

router-priority

router-priority *priority*

default router-priority

Purpose

Determines the preference for the Subscriber Management System (SMS) device to act as the designated router on a network.

Command Mode

OSPF interface configuration

Syntax Description

priority	Priority setting of the OSPF interface. The range of values is 0 to 255. The default value is 1.

Default

The priority value is 1.

Usage Guidelines

Use the **router-priority** command to determine the preference for the SMS device to act as the designated router on a network. Enter any value greater than 1 to indicate that the SMS device can act as the designated router. The router with the highest router priority will be used as the designated router for the network, if there is not a designated router already on the network. If two routers have the same router-priority value, the router with the higher router ID is the designated router for the network; see the **router-id** command.

Use the **default** form of this command to return the priority to the default value of 1.

Examples

The following example sets the router priority to 2:

```
[local]RedBack(config-ospf)#router-priority 2
```

Related Commands

router-id

show ip ospf

show ip ospf

Purpose

Displays Open Shortest Path First (OSPF) session information.

Command Mode

operator exec

Syntax Description

The **show ip ospf** command has several keyword constructs. Each construct each treated as a separate command. See the “Related Commands” section for a list of all **show ip ospf** commands.

Default

None

Usage Guidelines

Use the **show ip ospf** command with no keywords or arguments to display top-level OSPF session information.

See also these commands: **show ip ospf area**, **show ip ospf border router**, **show ip ospf database**, **show ip ospf interface**, **show ip ospf neighbor**, and **show ip ospf summary-range**.

Examples

The following example enables OSPF routing for the context named `customer`:

```
[customer]RedBack>show ip ospf

Context         RouterID        Precedence      External Precedence
customer        192.30.40.50    60              150

AreaCount       AreaBorderRtr   ASBoundaryRtr   TypeofService
1               No              Yes             TOS-Type0

SPFDelay(s)     SPFHoldTime(s)  SPFLastCompute  DefaultAllow[Metric]
5               0               03m12s          No [--]

Area List:
          1
```

The router ID is `192.30.40.50`. The OSPF precedence value is `60`. The type of service is normal. The Subscriber Management System (SMS) is configured as an autonomous system boundary router (ASBR) and one area is configured. The Shortest Path First (SPF) delay timer is five seconds, which is the interval between the receipt of a topology change and the start of the SPF calculation. The SPF hold time is `0`. The last SPF computation occurred `03m12s` (3 minutes 12 seconds) ago.

Related Commands

area
debug ip ospf
precedence
redistribute
router-id
show ip ospf area
show ip ospf border-router
show ip ospf database
show ip ospf interface
show ip ospf neighbor
show ip ospf summary-range
spf-timers
transmit-delay

show ip ospf area

show ip ospf area [*id* | *ip-address*] [**detail**]

Purpose

Displays information about an Open Shortest Path First (OSPF) area.

Command Mode

operator exec

Syntax Description

id	Optional. Area identifier. The range of values is 0 to 4,294,967,295.
ip-address	Optional. Area IP address.
detail	Optional. Lists details of configured areas.

Default

Displays summary information for all areas.

Usage Guidelines

Use the **show ip ospf area** command to display information on all areas. To view detailed information about a specific area, enter the *id* or *ip-address* argument. To view detailed information about all configured areas, enter only the **detail** keyword.

Examples

The following example displays area `1` information:

```
[local]RedBack>show ip ospf area 1

AreaID          InterfaceCount  AreaType
1               1               NORMAL
SPFCount        LinkStateUpdate
1               30m00s
VirtualLinks    DefaultRteCost  NssaTranslateRtr
0               N/A             ---

Interface List:
        10.1.1.1
```

Related Commands

area
areatype
debug ip ospf
ospf-interface
retransmit-interval
spf-timers

show ip ospf border-router

show ip ospf border-router

Purpose

Displays the routes to area border routers (ABRs) and autonomous system boundary routers (ASBRs).

Command Mode

operator exec

Syntax Description

The **show ip ospf** command has several keyword constructs. Each construct each treated as a separate command. See the "Related Commands" section for a list of all **show ip ospf** commands.

Default

None

Usage Guidelines

Use the **show ip ospf border-router** command to list information about routes to ABRs and ASBRs.

Examples

The following example indicates that there is a route to an ABR at IP address `10.1.1.2` with a host mask of 0xffffffff. The next hop IP address is `10.1.1.2`; the outgoing circuit is `10000001`; the outgoing interface IP address is `10.1.1.1`, and the route cost is `3`.

```
[local]RedBack>show ip ospf border-router

Type  Destination   Mask   NextHop    Circuit     OutIntf    Cost
ABR   10.1.1.3      32     10.1.1.3   10000001    10.1.1.1   3
ABR   10.1.1.2      32     10.1.1.2   10000001    10.1.1.1   3
ASBR  0.0.0.3       32     10.1.1.3   10000001    10.1.1.1   13
ASBR  0.0.0.3       32     10.1.1.2   10000001    10.1.1.1   13
ASBR  10.1.1.2      32     10.1.1.3   10000001    10.1.1.1   13
ASBR  10.1.4.2      32     10.1.1.2   10000001    10.1.1.1   13
```

Related Commands

cost
debug ip ospf
ospf-interface

show ip ospf database

show ip ospf database [[*id* | *ip-address*] [**external**] [**network**] [**nssa-ext**] [**router**] [**sum-asbr**] [**sum-net**] [*linkid linkadvrt*] | **database-summary**]]

Purpose

Displays entries in the Open Shortest Path First (OSPF) link-state database.

Command Mode

operator exec

Syntax Description

id	Optional. Area ID. The range of values is 0 to 4,294,967,295.
ip-address	Optional. IP address.
external	Optional. Displays all Type 5 AS-external link-state advertisements (LSAs).
network	Optional. Displays all network LSAs.
nssa-ext	Optional. Displays all Type 7 NSSA-external LSAs.
router	Optional. Displays all router LSAs.
sum-asbr	Optional. Displays all Type 4 summary-LSAs (routers).
sum-net	Optional. Displays all Type 3 summary-LSAs (networks).
linkid linkadvrt	Optional. Link identifier IP address (*linkid* argument) and advertising router IP address (*linkadvrt* argument). Used with the **external**, **network**, **nssa-ext**, **sum-asbr**, and **sum-net** keywords.
database-summary	Optional. Displays a count, by LSA type, of entries in the database. Also displays a checksum total.

Default

When this command is entered without any keywords, the system displays OSPF database summary information for all areas.

Usage Guidelines

Use the **show ip ospf database** command display entries in the OSPF link-state database.

Examples

The following example provides information about the LSA type, the link ID, and the advertising router IP address. In addition, link-state age, checksums, and sequence number information is included.

```
[local]RedBack>show ip ospf database

--------------------------------------------------------------------------------
                        AreaID 0
--------------------------------------------------------------------------------
Type      LinkID          AdvertisingRtr  Sequence#  ChkSum Option LsAge Length
Router    2.2.2.2         2.2.2.2         0x80000004 0xb99b E      1133  48
Router    1.1.1.1         1.1.1.1         0x80000005 0x2135 E      1093  48
Sum-Net   172.16.1.0      1.1.1.1         0x80000001 0xc6d3 E      1130  28
Sum-Net   100.1.0.0       1.1.1.1         0x80000001 0x32c0 E      1130  28
Sum-Net   192.168.2.0     1.1.1.1         0x80000002 0x8d5e E      1084  28

--------------------------------------------------------------------------------
                        AreaID 1
--------------------------------------------------------------------------------
Type      LinkID          AdvertisingRtr  Sequence#  ChkSum Option LsAge Length
Router    4.4.4.4         4.4.4.4         0x80000004 0x4b4e N/P    1133  48
Router    1.1.1.1         1.1.1.1         0x8000000a 0xa185 N/P    1093  60
Sum-Net   192.168.2.0     1.1.1.1         0x80000002 0x33b2 N/P    1084  28
Sum-Net   192.168.1.0     1.1.1.1         0x80000001 0x40a7 N/P    1130  28

--------------------------------------------------------------------------------
                        AreaID 2
--------------------------------------------------------------------------------
Type      LinkID          AdvertisingRtr  Sequence#  ChkSum Option LsAge Length
Router    1.1.1.1         1.1.1.1         0x80000007 0x149  N/P    1078  48
Router    3.3.3.3         3.3.3.3         0x80000007 0x350b N/P    1051  48
Sum-Net   100.1.0.0       1.1.1.1         0x80000001 0xd715 N/P    1088  28
Sum-Net   172.16.1.0      1.1.1.1         0x80000002 0x6a29 N/P    1082  28
Sum-Net   192.168.1.0     1.1.1.1         0x80000002 0x3ea8 N/P    1082  28
NSSA-Ext  172.16.11.0     3.3.3.3         0x80000001 0x4233 N/P     885  36
NSSA-Ext  3.3.3.3         3.3.3.3         0x80000001 0xb67a N/P    1051  36
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
                    Type-5 AS External
--------------------------------------------------------------------------------
Type      LinkID          AdvertisingRtr  Sequence#  ChkSum Option LsAge Length
External  172.16.11.0     1.1.1.1         0x80000001 0xf490 E      884   36
External  3.3.3.0         1.1.1.1         0x80000001 0x2b85 E      754   36
--------------------------------------------------------------------------------
```

The following example provides a summary of database information:

```
[local]RedBack>show ip ospf database database-summary

--------------------------------------------------------------------------
AreaID          Router  Network S-Net   S-ASBR  NSA-Ext Total    Checksum
--------------------------------------------------------------------------
0               2       0       3       0       0       5        0x261c1
1               2       0       2       0       0       4        0x1612c
2               2       0       3       0       2       7        0x2aee7
AS External                                             2        0x12015
--------------------------------------------------------------------------
```

The following example provides information specific to router LSAs:

```
[local]RedBack>show ip ospf database router

------------------------------------------------------------------------
                            AreaID 1
------------------------------------------------------------------------
Type      LinkID     AdvertisingRtr Sequence#   ChkSum  Option  LsAge
Router    10.1.1.2   10.1.1.2       0x8000000e  0x627d  E       36

LinkCount RouterBits
1         B
LinkType          LinkID      LinkData         NumTOS   Metric
Transit Network   10.2.1.2    10.2.1.1         0        1

------------------------------------------------------------------------
Type     LinkID     AdvertisingRtr Sequence#     ChkSum   Option  LsAge
Router   10.2.1.1   10.2.1.1       0x8000000d    0x6aa3   E      36

LinkCount RouterBits
1         B
LinkType          LinkID      LinkData         NumTOS   Metric
Transit Network   10.2.1.2    10.2.1.1         0        1
```

The following example provides information specific to network LSAs:

```
[local]RedBack>show ip ospf database network

------------------------------------------------------------------------
                              AreaID 1
------------------------------------------------------------------------
Type   LinkID   AdvertisingRtr Sequence#  ChkSum  Option  LsAge  Length
Router 10.2.1.2 10.1.1.2       0x8000000a 0x8c6b  E       32     737

RouterCount   Network Mask
2             255.255.255.0

Attached Routers:
    10.1.1.2
    10.2.2.1
```

The following example provides information specific to NSSA external LSAs:

```
[local]RedBack>show ip ospf database nssa-ext

-------------------------------------------------------------------------------
                  AreaID 2
-------------------------------------------------------------------------------

Type      LinkID          AdvertisingRtr  Sequence#  ChkSum Option LsAge Length
NSSA-Ext  172.16.11.0     3.3.3.3         0x80000001 0x4233 N/P    1401  36

NetworkMask     TOS        MetricType Metric     Tag        Forward
255.255.255.0   0          2          20         0          192.168.2.2
-------------------------------------------------------------------------------

Type      LinkID          AdvertisingRtr  Sequence#  ChkSum Option LsAge Length
NSSA-Ext  3.3.3.3         3.3.3.3         0x80000001 0xb67a N/P    1567  36

NetworkMask     TOS        MetricType Metric     Tag        Forward
255.255.255.255 0          2          20         0          192.168.2.2
-------------------------------------------------------------------------------
```

The following example provides information specific to summary network LSAs, a link ID of `10.1.1.0`, with an advertising router at IP address `10.1.1.2`:

```
[local]RedBack>show ip ospf database sum-net 10.1.1.0 10.1.1.2

-------------------------------------------------------------------
                              AreaID 1
-------------------------------------------------------------------
Type    LinkID   AdvertisingRtr Sequence#  ChkSum  Option Length LSAge
Sum-Net 10.1.1.0 10.1.1.2       0x8000000c 0x45c8  E      741    28
OriginArea      NetworkMask     TOS       Metric
N/A             255.255.255.0   0         10
```

Related Commands

area
debug ip ospf
router-id
transmit-delay

show ip ospf interface

show ip ospf interface [*ip-address* | **detail**]

Purpose

Displays OSPF interface information.

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address of the interface.
detail	Optional. Lists all OSPF interfaces.

Default

Displays summary information for all OSPF interfaces.

Usage Guidelines

Use the **show ip ospf interface** command with no keywords or arguments to display summary information. Specify an IP address to view information about a specific OSPF interface, or list detailed information for all OSPF interfaces by using the **detail** keyword.

Examples

The following example displays interface IP addresses, netmasks, network types (in this case broadcast), cost, priority, state (in this case, initial) and the area ID.

```
[local]RedBack>show ip ospf interface

-----------------------------------------------------------------------
Address        Mask  NetworkType  Cost   Priority  State    AreaID
-----------------------------------------------------------------------
192.30.40.60   24    Broadcast    1      0         Initial  1
```

The following example displays information specific to the interface at IP address `192.30.40.60` is displayed, including the router ID and the type of network to which the interface is attached. Neighbors of the interface are listed. Interface timer configuration, authentication, designated router, and backup designated router information is displayed.

```
[local]RedBack>show ip ospf interface 192.30.40.60

Address         Netmask         AreaID          RouterID
192.30.40.60    255.255.255.0   1               192.30.40.60

NetworkType     State           Cost            Priority
Broadcast       Initial         1               0

TransmitDelay   HelloInterval   DeadInterval    RetransmitInterval
01s             10s             40s             5s

DesignatedRtrID DesignatedRtrIP BackupRtrID     BackupRtrIP
0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0

ACKDelay        Authentication  NeighborCount   MTU
2               Simple          1               0

Neighbor List:
   192.40.50.61
```

Related Commands

area
authentication
cost
debug ip ospf
hello-interval
ospf-interface
router-id
routerdead-interval

show ip ospf neighbor

show ip ospf neighbor [*id* | **detail**]

Purpose

Displays OSPF neighbor information.

Command Mode

operator exec

Syntax Description

id	Optional. Router ID (IP address).
detail	Optional. Lists all OSPF neighbors.

Default

Displays summary information for all neighbors.

Usage Guidelines

Use the **show ip ospf neighbor** command with no keywords or arguments to view summary information. To view information about a specific neighbor, enter the router ID of the neighbor. To view all neighbors, use only the **detail** keyword.

Examples

The following example provides information on the peer:

```
[local]RedBack>show ip ospf neighbor

NeighborID    NeighborAddress  Pri   State    Interface
10.1.1.2      10.2.1.2         1     Full/DR  10.2.1.1
```

The following example provides information specific to the peer with the router ID of `10.1.1.2`:

```
[local]RedBack>show ip ospf neighbor 10.1.1.2

Address          RouterID    State        Priority
10.2.1.2         10.1.1.2    Full         1

DesignatedRtrID  BackupRtrID Interface    Area
10.2.1.2         0.0.0.0     10.2.1.1     1
```

The following example lists information about all neighbors:

```
[local]RedBack>show ip ospf neighbor detail

-----------------------------------------
             Neighbor 10.1.1.2
-----------------------------------------
Address           RouterID    State       Priority
10.2.1.2          10.1.1.2    Full        1
DesignatedRtrID   BackupRtrID Interface   Area
10.2.1.2          0.0.0.0     10.2.1.1    1
```

Related Commands

area
debug ip ospf
ospf-interface
router-id

show ip ospf summary-range

show ip ospf summary-range [**area** [*area-id*] | **as** | **nssa** [*area-id*]] [*ip-address netmask*]]

Purpose

Displays the summary ranges for Open Shortest Path First (OSPF) areas, autonomous systems, and not-so-stubby-areas (NSSAs).

Command Mode

operator exec

Syntax Description

area	Optional. Displays area summary ranges.
area-id	Optional. Area ID. The ID can be either numeric, an IP address, or a summary range IP address. The range of numeric values is 0 to 4,294,967,295. The default numeric value is 0.
ip-address netmask	Optional. Summary range address and netmask.
as	Optional. Displays only autonomous system (AS) summary ranges.
nssa	Optional. Displays only NSSA summary ranges.

Default

When this command is entered without any optional keywords, the system displays configured summary ranges for all areas, ASs, and NSSAs.

Usage Guidelines

Use the **show ip ospf summary-range** command to display the summary ranges for OSPF areas, autonomous systems, and NSSAs.

Examples

The following example displays a list of configured summary ranges for all areas and autonomous systems:

```
[local]RedBack>show ip ospf summary-range

-----------------------------------------
Summary-Range   AreaID          Number
```

```
-----------------------------------------
AS-Sumrange     N/A             1
Area-Sumrange   1               0
Area-Sumrange   2               0
NSSA-Sumrange   1               0
NSSA-Sumrange   2               1
-----------------------------------------
```

The following example displays information on summary ranges for all areas:

```
[local]RedBack>show ip ospf summary-range area

-------------------------------------------------------------------------
Summary-Range[AreaID]   Address     Mask            Options   NumRoutes
Area 3                  10.1.1.1    255.255.255.0   ---       0
-------------------------------------------------------------------------
```

The following example displays information on summary ranges for all autonomous systems:

```
[local]RedBack>show ip ospf summary-range as

-------------------------------------------------------------------------
Summary-Range[AreaID]   Address     Mask            Options   NumRoutes
AS                      10.2.0.0    255.255.255.0   ---       0
-------------------------------------------------------------------------
```

The following example provides information specific to NSSA summary ranges.

```
[local]RedBack>show ip ospf summary-range nssa

-------------------------------------------------------------------------------
Summary-Range[AreaID] Address         Mask            Options      NumRoutes
NSSA 2                3.3.3.0         255.255.255.0   ---          1
-------------------------------------------------------------------------------
```

The following example displays NSSA 2, which has a database entry of `3.3.3.3 255.255.255.0`. Due to the configuration of the summary range, the ABR originates an external Type 5 LSA route `3.3.3.0 255.255.255.0` into the backbone area.

```
[local]RedBack>show ip ospf summary-range nssa 3.3.3.0 255.255.255.0

-------------------------------------------------------------------------------
Summary-Range[AreaID] Address         Mask            Options      NumRoutes
NSSA 2                3.3.3.0         255.255.255.0   ---          1

Covered Database Entries:
        Type      LinkID          AdvertisingRtr
        NSSA-Ext  3.3.3.3         3.3.3.3
-------------------------------------------------------------------------------
```

Related Commands

area-sumrange
as-sumrange
nssa-sumrange

spf-timers

spf-timers {*spf-delay spf-holdtime*}

{**no** | **default**} **spf-timers**

Purpose

Configures the delay time between the receipt of a topology change and the start of the Shortest Path First (SPF) calculation. Also determines the hold time between two consecutive SPF calculations.

Command Mode

OSPF configuration

Syntax Description

spf-delay	Delay time, in seconds, between the receipt of a topology change and the start of the SPF calculation. The range of values is 0 to 4,294,967,295. The default value is 5. A value of 0 means that the SPF calculation is started immediately.
spf-holdtime	Minimum time, in seconds, between two consecutive SPF calculations. The range of values is 0 to 4,294,967,295. The default value is 10. A value of 0 means that with two consecutive SPF calculations, only one is constrained by the delay.

Default

The *spf-delay* value is 5 seconds. The *spf-holdtime* value is 10 seconds.

Usage Guidelines

Use the **spf-timers** command to tune the rate at which OSPF topology changes and recalculations take place. Setting the delay and hold times to low values enables faster switching to an alternate path in the event of failure. However, it consumes more CPU processing time.

Use the **no** or **default** form of this command to return the delay and holdtime values to their default settings.

Examples

The following example sets the SPF delay and holdtimes to 2 and 5:

```
[local]RedBack(config-ospf)#spf-timers 2 5
```

Related Commands

debug ip ospf
show ip ospf
show ip ospf database

transmit-delay

transmit-delay *delay*

{**no** | **default**} **transmit-delay**

Purpose

Configures the amount of time by which the Open Shortest Path First (OSPF) interface increases the age of link-state update packets.

Command Mode

OSPF interface configuration

Syntax Description

delay	The amount of time, in seconds, by which the OSPF interface increases the age of link-state update packets. The range of values is 1 to 65,535. The default value is 1.

Default

The delay value is one second.

Usage Guidelines

Use the **transmit-delay** command to configure the amount of time by which the OSPF interface increases the age of link-state update packets. Before a link-state update packet is sent out an interface, the OSPF interface must increase the age of the packet. On a slow link, for example, one with an average propagation delay of multiple seconds, the age of the link-state update packet must be increased by a similar delay interval. Configuring the delay ensures that you do not receive a packet that is younger than the original copy.

Use the **no** or **default** form of this command to return the interval value to its default setting.

Examples

The following example sets the transmit delay at 3 seconds:

```
[local]RedBack(config-ospf-interface)#transmit-delay 3
```

Related Commands

debug ip ospf
show ip ospf interface

BGP Commands

This chapter describes the commands used to configure and maintain Border Gateway Protocol (BGP) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure BGP, and configuration examples, see the “Configuring BGP” chapter in the *Access Operating System (AOS) Configuration Guide*.

accept-med

accept-med

no accept-med

Purpose

Allows the import of the Multi-Exit Discriminator (MED) attribute from external peers, enabling the Subscriber Management System (SMS) device to select the optimal exit point among multiple points to a remote autonomous system.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

This command has no arguments or keywords.

Default

The MED attribute from external peers is stripped off and ignored.

Usage Guidelines

Use the **accept-med** command to allow the import of the MED attribute from external peers, enabling the SMS device to select the optimal exit point among multiple points to a remote autonomous system. On external BGP links, if all other factors in determining an exit point are equal, the exit point with the lowest MED metric is preferred. This command has no effect on an internal BGP peer, because a received MED value is always retained on an internal connection.

To allow the import of the MED attribute from external peers to a BGP group, enter this command in BGP group configuration mode. To allow import to a BGP peer, enter this command in BGP peer configuration mode.

Use the **no** form of this command to return the BGP to the default behavior of rejecting the MED attribute from external peers.

Examples

The following example configures the group `customer` in BGP autonomous system number `64001` to accept the MED attribute from external peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer remote-as 11
[local]RedBack(config-group)#accept-med
```

The following example enables the peer at IP address `192.33.20.1` to accept the MED attribute from external peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer remote-as 11
[local]RedBack(config-group)#neighbor 192.33.20.1
[local]RedBack(config-peer)#accept-med
```

Related Commands

always-compare-med
metric-out
show ip bgp

aggregate-address

aggregate-address *ip-address netmask* [**summary-only**] [**as-set**]

no aggregate-address *ip-address netmask*

Purpose

Creates an aggregate entry in the Border Gateway Protocol (BGP) routing table when there are more-specific BGP routes available in the specified range.

Command Mode

BGP configuration

Syntax Description

ip-address	Aggregate address.
netmask	Aggregate netmask.
summary-only	Optional. Filters all more-specific routes from updates.
as-set	Optional. Generates autonomous system set path information.

Default

No aggregation is performed.

Usage Guidelines

Use the **aggregate-address** command to create an aggregate entry in the BGP routing table when there are more-specific BGP routes available in the specified range. When a BGP speaker receives a prefix with the atomic-aggregate attribute set, it must not take the prefix and deaggregate it into any more-specific entries in BGP. By default, the atomic-aggregate attribute is set unless you specify the **as-set** keyword.

The **as-set** keyword creates an aggregate entry as described above, but the path advertised for this route will be an AS set consisting of all elements in all paths that are being summarized.The **summary-only** keyword suppresses advertisements of more specific routes to all neighbors.

Use the **no** form of this command to remove the specified aggregate address.

Examples

The following example configures an aggregate address for BGP autonomous system number (ASN) 4. The path advertised for this route is an AS set consisting of all elements contained in all paths that are being summarized.

```
[local]RedBack(config-ctx)#router bgp 4
[local]RedBack(config-bgp)#aggregate-address 194.0.0.0 255.0.0.0 as-set
```

Related Commands

no-aggregator-id
show ip bgp paths

allow-bad-routerid

allow-bad-routerid

no allow-bad-routerid

Purpose

Allows Border Gateway Protocol (BGP) sessions with peers that have invalid router IDs.

Command Mode

BGP peer configuration

Syntax Description

This command has no keywords or arguments.

Default

BGP sessions with peers that have invalid router IDs are not allowed.

Usage Guidelines

Use the **allow-bad-routerid** command to allow BGP sessions with peers that have invalid router IDs. The router ID cannot be IP address 0.0.0.0 or 255.255.255.255.

Use the **no** form of this command to disable the ability to allow sessions with peers that have invalid router IDs.

Examples

The following example enables the peer at IP address `10.10.1.1` to have BGP sessions with peers that have invalid router IDs:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer remote-as 11
[local]RedBack(config-group)#neighbor 10.10.1.1
[local]RedBack(config-peer)#allow-bad-routerid
```

Related Commands

router-id
show ip bgp

always-compare-med

always-compare-med

no always-compare-med

Purpose

Enables the comparison of the Multi-Exit Discriminator (MED) attribute for paths from peers in different autonomous systems.

Command Mode

BGP configuration

Syntax Description

This command has no arguments or keywords.

Default

The Access Operating System (AOS) only compares MED attributes for paths from external peers that are in the same autonomous system.

Usage Guidelines

Use the **always-compare-med** command to enable the comparison of the MED attribute for paths from peers in different autonomous systems. MED value provides information to external peers about the preferred path into an autonomous system when it has multiple entry points. A lower value is preferred over a higher value.

Use the **no** form of this command to disable comparison of MED attributes for paths from neighbors in different autonomous systems.

Examples

The following example configures BGP autonomous system number (ASN) `64001` to compare MEDs among alternative paths, regardless of the autonomous system from which the paths are received:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#always-compare-med
```

Related Commands

accept-med
metric-out
show ip bgp

clear ip bgp

clear ip bgp {*ip-address* | **all** | **group** *name* [**soft** [**in** | **out**]]}

Purpose

Resets a Border Gateway Protocol (BGP) neighbor connection or applies changes to BGP parameters without dropping the connection.

Command Mode

administrator exec

Syntax Description

ip-address	IP address of the BGP peer.
all	Clears connections to all peers.
group *name*	Name of the group in which all BGP peer connections are cleared.
soft	Optional. Does not drop the BGP connection, but applies any changes to BGP parameters to the connection. If the **soft** keyword is not specified, the BGP connection is dropped immediately.
in	Optional. Applies new routing policies to inbound connections only. Used only with the **soft** keyword. If the **in** or **out** optional keyword is not specified, changes to BGP parameters are applied to both inbound and outbound connection.
out	Optional. Applies new routing policies to outbound connections only. Used only with the **soft** keyword. If the **in** or **out** optional keyword is not specified, changes to BGP parameters are applied to both inbound and outbound connections.

Default

None

Usage Guidelines

Use the **clear ip bgp** command to reset a BGP neighbor connection, or to apply changes to BGP parameters to the connection without causing a hard reset (which drops the connection immediately). This command is typically used to apply new parameters, such as inbound and outbound routing policies, to a BGP neighbor connection. Changes to these parameters are not applied to the connection until the **clear ip bgp** command is issued.

Caution You must specify the **soft** keyword if you do not want the BGP neighbor connection dropped. A hard reset can impact network connectivity. Only use a hard reset as a last resort.

Examples

The following example causes a hard reset in which the connection to the BGP neighbor at IP address `10.11.48.170` is immediately dropped:

```
[local]RedBack#clear ip bgp 10.11.48.170

 Jan 5 19:32:02: %BGP-6-INFO: 10.11.48.170 DOWN - User action
 Jan 5 19:32:07: %BGP-6-INFO: 10.11.48.170 UP
```

The following example enables any BGP parameter changes to be applied to outbound connections without dropping the connection with the neighbor at IP address `10.11.48.170`:

```
[local]RedBack#clear ip bgp 10.11.48.170 soft out
```

Related Commands

debug ip bgp
group
maximum-prefix
neighbor
show ip bgp
show ip bgp groups
show ip bgp neighbors

client-to-client

client-to-client

no client-to-client

Purpose

Disables route reflection between clients in the same internal Border Gateway Protocol (I-BGP) group.

Command Mode

BGP group configuration

Syntax Description

This command has no keywords or arguments.

Default

Routes are reflected between I-BGP clients.

Usage Guidelines

Use the **client-to-client** command to disable route reflection between clients in the same I-BGP group. This command is available only if the group is configured as an I-BGP group. An I-BGP group has the same ASN as the local ASN specified in the **router bgp** *asn* command construct. An example of when a network administrator may not want routes learned from a client to be reflected to other clients is the case where two peers may already have their own BGP connection established.

Use the **no** form of this command to re-enable client-to-client reflection.

Examples

The following example disables client-to-client reflection between clients in the group called `customer1`:

```
[local]RedBack(config-ctx)#router bgp 2
[local]RedBack(config-bgp)#group customer1 remote-as 2
[local]RedBack(config-group)#no client-to-client
```

Related Commands

cluster-id
route-reflector-client

cluster-id

cluster-id *id*

no cluster-id

Purpose

Specifies the route reflector cluster ID for the Border Gateway Protocol (BGP) routing process.

Command Mode

BGP configuration

Syntax Description

id	Cluster identifier, in 4-byte format. The range of values is 1 to 4,294,967,295. By default, the router ID is used as the cluster ID.

Default

The router ID is used as the route reflector cluster ID.

Usage Guidelines

Use the **cluster-id** command to specify the route reflector cluster ID for the BGP routing process. If a route reflector cluster has more than one route reflector, all route reflectors in the cluster must be configured with the same 4-byte cluster ID. The common cluster ID allows one route reflector to recognize updates from other route reflectors in the same cluster.

Use the **no** form of this command to remove the cluster ID.

Examples

The following example configures a cluster ID of `100` for BGP autonomous system number (ASN) `64001`:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#cluster-id 100
```

Related Commands

route-reflector-client
show ip bgp

debug ip bgp

debug ip bgp [**all** | **events** | **keepalives** | **misc** | **packets** | **updates**]

no debug ip bgp

Purpose

Enables the logging of Border Gateway Protocol (BGP) debug messages.

Command Mode

administrator exec

Syntax Description

all	Optional. Enables the logging of debug messages for all BGP events.
events	Optional. Enables the logging of debug messages for BGP non-update events.
keepalives	Optional. Enables the logging of debug messages for BGP keepalive packet events.
misc	Optional. Enables the logging of debug messages for miscellaneous BGP events.
packets	Optional. Enables the logging of debug messages for all BGP packet events.
updates	Optional. Enables the logging of debug messages for BGP update packet events.

Default

Disabled

Usage Guidelines

Use the **debug ip bgp** command to enable the logging of BGP debug messages.

Use the **logging console** and **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable the logging of BGP debugging messages.

Examples

The following example enables the logging of debug messages for all BGP packet events:

```
[local]RedBack#debug ip bgp packets
```

Related Commands

clear ip bgp
logging console
show ip bgp
terminal monitor

default-originate

default-originate

no default-originate

Purpose

Sends the default route (0.0.0.0) to Border Gateway Protocol (BGP) peers.

Command Mode

BGP group configuration

Syntax Description

This command has no arguments or keywords.

Default

No default route is sent to peers.

Usage Guidelines

Use the **default-originate** command to send the default route (0.0.0.0) to BGP peers. This command does not require the presence of route 0.0.0.0 in the routing table.

Use the **no** form of this command to remove the default route.

Examples

The following example sends the default route (0.0.0.0) to peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer remote-as 11
[local]RedBack(config-group)#default-originate
```

Related Commands

show ip bgp paths

enable-peer

enable-peer

no enable-peer

Purpose

Enables a Border Gateway Protocol (BGP) peer administratively.

Command Mode

BGP peer configuration

Syntax Description

This command has no arguments or keywords.

Default

A peer is administratively disabled.

Usage Guidelines

Use the **enable-peer** command to enable a peer administratively. A BGP peer session is not initiated or accepted unless the peer has been enabled with this command. Use this command in conjunction with the **neighbor** command in BGP group configuration mode.

Use the **no** form of this command to disable the peer.

Examples

The following example enables the peer at IP address `10.10.1.1` administratively:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer remote-as 11
[local]RedBack(config-group)#neighbor 10.10.1.1
[local]RedBack(config-peer)#enable-peer
```

Related Commands

neighbor
show ip bgp neighbors

export-non-active

export-non-active

no export-non-active

Purpose

Configures the specified Border Gateway Protocol (BGP) routing process to consider the local, nonactive BGP routes for export to peers when the active route is prohibited from being exported.

Command Mode

BGP configuration

Syntax Description

This command has no arguments or keywords.

Default

The BGP routing process considers exporting the best local, nonactive BGP route to peers.

Usage Guidelines

Use the **export-non-active** command to configure the specified BGP routing process to consider local, nonactive BGP routes for export to peers when the active route is prohibited from being exported.

Use the **no** form of this command to configure the BGP routing process to ignore local, nonactive BGP routes for export to peers.

Examples

The following example configures BGP autonomous system number (ASN) `64001` to consider local, nonactive BGP routes to export to peers when the active route is prevented (by routing policy) from being exported:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#export-non-active
```

Related Commands

show ip bgp paths
route-map

group

group *name* [**confederation**] **remote-as** *asn*

no group *name*

Purpose

Configures Border Gateway Protocol (BGP) group and enters BGP group configuration mode.

Command Mode

BGP configuration

Syntax Description

name	Name of the group.
confederation	Optional. Groups peers that belong to the same confederation.
remote-as *asn*	Specifies either the remote autonomous system number (ASN), or (if the **confederation** keyword is used) indicates the routing domain identifier. The range of values is 1 to 65,535.

Default

There are no preconfigured BGP groups.

Usage Guidelines

Use the **group** command to configure a BGP group and enter BGP group configuration mode. Parameters configured in BGP group configuration mode are applied to all peer members that belong to the group.

An internal BGP (I-BGP) group has the same ASN as the local ASN specified in the **router bgp** *asn* command construct. An external (E-BGP) group has a different ASN from the local autonomous system, and is not part of a confederation.

The **confederation** keyword is only available if you have used the optional **routing-domain** *id* construct with the **router bgp** command. Use the **confederation** keyword to configure an I-BGP group as part of a discrete routing domain within an autonomous system.

Use the **no** form of this command to remove the specified group.

Examples

The following example configures peers in the group called `customer1` to be part of ASN `50`:

```
[localRedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1 remote-as 50
[local]RedBack(config-group)#
```

The following example configures peers in the group named `customer2` to be part of a confederation with a routing domain identifier of `100`:

```
[localRedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer2 confederation remote-as 100
[local]RedBack(config-group)#
```

Related Commands

router bgp
neighbor
show ip bgp groups

hold-time

hold-time *holdtime*

no hold-time

Purpose

Sets the maximum interval allowed by the Border Gateway Protocol (BGP) peer or group between successive keepalive or update messages sent by a remote peer before the Subscriber Management System (SMS) device drops the BGP session.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

holdtime	Maximum amount of time, in seconds, allowed between successive keepalive or update messages. The range of values is 0 to 21,845. The default value is 180.

Default

The hold time is 180 seconds.

Usage Guidelines

Use the **hold-time** command to configure the maximum interval allowed by the BGP peer or group between successive keepalive messages or update messages sent by a remote peer before the SMS device drops the BGP session.

To apply a hold time value to a group, enter this command in BGP group configuration mode. To set a hold time value for a peer, enter this command in BGP peer configuration mode.

Use the **no** form of this command to return the hold time to its default value.

Examples

The following example sets the hold time for the group called `customer1` to `160` seconds:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#hold-time 160
```

The following example sets the hold time for the BGP peer at IP address `192.30.12.10` to `160` seconds:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-group)#neighbor 192.30.12.10
[local]RedBack(config-peer)#hold-time 160
```

Related Commands

maximum-prefix
show ip bgp

maximum-prefix

maximum-prefix *max-prefix*

no maximum-prefix

Purpose

Sets the maximum number of prefixes that are accepted from a peer before the Border Gateway Protocol (BGP) session is dropped by the Subscriber Management System (SMS) device.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

max-prefix	Maximum number of prefixes allowed from a BGP peer. The range of values is 1 to 4,294,967,295. The default value is unlimited.

Default

An unlimited number of prefixes are accepted.

Usage Guidelines

Use the **maximum-prefix** command to set the maximum number of prefixes that are accepted from a peer before the BGP session is dropped by the SMS device. When the peer is terminated, the peer stays down until the **clear ip bgp** command is issued.

To enable a maximum setting for a group, use this command in BGP group configuration mode. To apply a maximum setting to a peer, enter this command in BGP peer configuration mode.

Use the **no** form of this command to return the maximum number of prefixes to unlimited.

Examples

The following example terminates the BGP peer session if more than `20000` prefixes are sent by the offending peer to the group called `customer`:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#maximum-prefix 20000
```

The following example terminates the BGP peer session if more than 20000 prefixes are sent by the offending peer to the peer at IP address 192.20.12.10:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#maximum-prefix 20000
```

Related Commands

clear ip bgp
maximum-prefix-warn
show ip bgp paths

maximum-prefix-warn

maximum-prefix-warn *threshold*

no maximum-prefix-warn

default maximum-prefix-warn

Purpose

Sets the number of prefixes that are accepted from a peer during a Border Gateway Protocol (BGP) session before a warning is issued.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

threshold	Number of prefixes that are accepted before a warning is issued. The range of values is 1 to 4,294,967,295. The default value is 4,294,967,295.

Default

Because the number of prefixes allowed is virtually unlimited, no warnings are issued.

Usage Guidelines

Use the **maximum-prefix-warn** command to set the number of prefixes that are accepted from a peer during a BGP session before a warning is issued. When this command is enabled, the specified BGP group or peer receives a warning once the number of prefixes exceeds the configured threshold.

To apply a warning threshold to a group, enter this command in BGP group configuration mode. To apply a warning threshold to a peer, enter this command in BGP per configuration mode.

Use the **no** form of this command to disable warnings.

Use the **default** form of this command to reset the warning threshold to the default value of 4,294,967,295.

Examples

The following example issues a warning message if the offending peer sends more than `15000` prefixes to the group called `customer`:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#maximum-prefix-warn 15000
```

The following example issues a warning message if the offending peer sends more than `15000` prefixes to the peer at IP address `192.20.12.10`:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#maximum-prefix-warn 15000
```

Related Commands

clear ip bgp
maximum-prefix
show ip bgp paths

metric-out

metric-out *metric*

no metric-out

Purpose

Configures the Multi-Exit Discriminator (MED) attribute value that the specified Border Gateway Protocol (BGP) group sends to peers that are external to the autonomous system. The MED attribute is sent to external peers in update messages.

Command Mode

BGP group configuration

Syntax Description

metric MED value to send to external peers. The range of values is 0 to 4,294,967,295. The default value is 4,294,967,295.

Default

The MED attribute is not sent to external peers. When this command is enabled, the MED attribute value is 4,294,967,295.

Usage Guidelines

Use the **metric-out** command to configure the MED attribute value a BGP group sends to peers that are external to the autonomous system. The MED path attribute enables the Subscriber Management System (SMS) device to select the optimal exit point (among multiple points) to a remote autonomous system. If all other factors in determining an exit point are equal, the exit point with the lowest MED attribute is preferred. If a MED attribute is received over an external BGP link, it is propagated over internal links within the autonomous system.

The MED value can also be set using the **set metric** command in route map configuration mode and by applying the **metric** keyword with the **redistribute** command in BGP configuration mode.

Use the **no** form of this command to return the BGP to the default behavior of not sending the MED attribute to external peers.

Examples

The following example configures the group called `customer` to send all routes to external peers using a MED attribute value of 2:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#metric-out 2
```

Related Commands

accept-med
redistribute
set metric
show ip bgp paths

neighbor

neighbor *ip-address*

no neighbor *ip-address*

Purpose

Configures the Border Gateway Protocol (BGP) peer IP address and enters BGP peer configuration mode.

Command Mode

BGP group configuration

Syntax Description

ip-address	IP address of the BGP peer.

Default

There are no preconfigured BGP peers.

Usage Guidelines

Use the **neighbor** command to configure the BGP peer IP address and to enter BGP peer configuration mode.

You must also enable the peer through the **enable-peer** command in BGP peer configuration mode.

Use the **no** form of this command to remove the specified peer.

Examples

The following example configures the remote peer at IP address `162.5.7.24` as part of the group called `customer`, and enables the remote peer:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#neighbor 162.5.7.24
[local]RedBack(config-peer)#enable-peer
```

Related Commands

enable-peer
show ip bgp neighbors

nexthop-self

nexthop-self

no nexthop-self

Purpose

Forces the Border Gateway Protocol (BGP) not to send third party next-hop information to peers.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

This command has no arguments or keywords.

Default

Third party next-hop information is sent when appropriate.

Usage Guidelines

Use the **nexthop-self** command to disable the BGP routing process from sending third party next-hop information. This type of information is appropriate to send, for example, when routes are propagated between two peers on a common subnet.

To disable a group from sending third party next-hop information to peers, use this command in BGP group mode. To disable a peer from sending this information, use this command in BGP peer configuration mode.

Use the **no** form of this command to return BGP to the default behavior of sending third-party next-hop information when appropriate.

Examples

The following example configures the group called `customer1` not to send third-party next-hop information to peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#nexthop-self
```

The following example configures the peer at IP address 192.30.12.10 not to send third-party next-hop information to peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#nexthop-self
```

Related Commands

show ip bgp paths

no-aggregator-id

no-aggregator-id

no no-aggregator-id

Purpose

Sets the router ID in the Border Gateway Protocol (BGP) aggregator path attribute to zero, thereby preventing routers within an autonomous system from creating aggregate routes that contain disparate AS paths.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

This command has no arguments or keywords.

Default

The local router ID is included in the BGP aggregator path attribute.

Usage Guidelines

Use the **no-aggregator-id** command to set the router ID in the BGP aggregator path attribute to 0, thereby preventing routers within an autonomous system from creating aggregate routes that contain disparate AS paths.

To apply a router ID value of 0 to a group, enter this command in BGP group configuration mode. To apply the value to a peer, use this command in BGP peer configuration mode.

Use the **no** form of this command to return BGP to the default behavior of including the local router ID in the BGP aggregator path attribute.

Examples

The following example configures the group called `customer1` to send a router ID of `0` as its BGP aggregator path attribute:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#no-aggregator-id
```

The following example configures the peer at IP address `192.20.12.10` to send a router ID of 0 as its BGP aggregator path attribute:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#no-aggregator-id
```

Related Commands

aggregate-address
show ip bgp paths

out-delay

out-delay *delay*

no out-delay

Purpose

Determines how long a route must be present in the routing table before being exported to the Border Gateway Protocol (BGP) routing process.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

delay	Output delay time, in seconds. The range of values is 0 to 65,535. The default value is 0.

Default

There is no set time that routes must be present in the routing table before being exported to the BGP routing process.

Usage Guidelines

Use the **out-delay** command to specify the number of seconds a route must be in the routing table before being exported to the BGP routing process. This command allows a limited form of route flap dampening. If you omit this command, routes are exported to BGP immediately after they have been added to the routing table.

To set the output delay time for routes associated with a group, enter this command in BGP group configuration mode. To apply the output delay time to routes associated with a peer, use this command in BGP peer configuration mode.

Use the **no** form of this command to return to determine that routes do not need to be present for any set period of time in the routing table before they are exported to the BGP routing process.

Examples

The following example ensures that a route associated with the group called `customer1` must be in the local routing table for at least `15` seconds before it is exported to BGP:

```
[[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#out-delay 15
```

The following example ensures that a route associated with the peer at IP address `192.20.12.10` must be in the local routing table for at least `15` seconds before it is exported to BGP:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#out-delay 15
```

Related Commands

export-non-active
show ip bgp paths

passive

passive

no passive

Purpose

Prevents the sending of active open messages to peers for initiation of a Border Gateway Protocol (BGP) connection.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

This command has no arguments or keywords.

Default

Active open messages are sent to all administratively enabled peers.

Usage Guidelines

Use the **passive** command to prevent the initiation of BGP connections to peers. This allows the Access Operating System (AOS) to wait for a peer to initiate a BGP session. If both ends of a BGP session are configured to be passive, no BGP session is established.

To prevent members of a group from initiating a BGP session, use this command in BGP group configuration mode. To prevent individual peers from initiating sessions, enter this command in BGP peer configuration mode.

Use the **no** form of this command to return BGP to its default behavior.

Examples

The following example ensures that no active open messages are sent by the group called `customer` to peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#passive
```

The following example ensures that no active open messages are sent by the peer at IP address `192.20.12.10` to its peers:

```
[local]RedBack(config-ctx)#router bgp 64001
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#passive
```

Related Commands

show ip bgp

precedence

precedence *prec*

no precedence

Purpose

Sets the precedence for routes learned from the Border Gateway Protocol (BGP).

Command Mode

BGP configuration
BGP group configuration
BGP peer configuration

Syntax Description

prec	Precedence value. The range of values is 10 to 255. The default value is 170. A lower value indicates a more-preferred route.

Default

Routes learned from BGP have a value of 170.

Usage Guidelines

Use the **precedence** command to modify the precedence value of routes learned from BGP. A lower value indicates a more-preferred route. When configuring routes for multiple protocols, ensure that the *value* argument for each route type is distinct from the other. For example, ensure that the *value* argument for BGP routes is distinct from static IP routes, which must also be distinct from Open Shortest Path First (OSPF) routes. The Access Operating System (AOS) assigns a default value to each routing protocol process.

Table 34-1 lists the default precedence value for each protocol:.

Table 34-1 Protocol Precedence Defaults

Protocol	Precedence Value
Directly connected	0
Static IP	10
Subscriber record	15
OSPF—Internal to the autonomous system	60
Routing Information Protocol (RIP)	100
OSPF—External to the autonomous system	150
BGP	170

Use the **no** form of this command to return the BGP precedence value to the default value of 170.

Examples

The following example sets the precedence for BGP autonomous system number (ASN) `321 to 195`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#precedence 195
```

The following example sets the BGP precedence for the group called `customer1` to `195`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#precedence 195
```

The following example sets the BGP precedence for the peer at IP address `192.20.12.10` to `195`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#precedence 195
```

Related Commands

ip route—context configuration mode
precedence—OSPF configuration mode
precedence—RIP configuration mode
preference
show ip bgp paths

preference

preference *pref*

no preference

Purpose

Determines the preferred route when two or more routes learned from Border Gateway Protocol (BGP) have the same precedence value, which is set by the **precedence** command.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

pref	Preference value. The range of values is 0 to 65,535. The default value is 0.

Default

The preference value is 0.

Usage Guidelines

Use the **preference** command to break a tie, in the case where two or more routes learned from BGP have the same precedence value, which is set by the **precedence** command.

Use the **no** form of this command to return BGP to the default **preference** value of 0.

Examples

The following example ensures that, for the group called `customer1`, routes learned from peers have a preference value of `50`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#preference 50
```

The following example ensures that, for the peer at IP address `192.20.12.10`, routes learned from peers have a preference value of `50`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#preference 50
```

Related Commands

precedence—BGP group and BGP peer configuration modes
show ip bgp paths

redistribute

redistribute {**direct** | **ospf** | **rip** | **static** | **subscriber**} [**route-map** *map-name*] [**metric** *metric*]

no redistribute {[**direct** | **ospf** | **rip** | **static** | **subscriber**} [**route-map** *map-name*] [**metric** *metric*]

Purpose

Redistributes routes learned through other protocols and sources into the Border Gateway Protocol (BGP) routing process.

Command Mode

BGP configuration

Syntax Description

direct	Redistributes routes from directly attached networks into BGP.
ospf	Redistributes routes from the Open Shortest Path First (OSPF) routing process into the BGP domain.
rip	Redistributes routes from the Routing Information Protocol (RIP) into BGP.
static	Redistributes static routes into BGP.
subscriber	Injects routes configured within subscriber records.
route-map *map-name*	Optional. Applies a route map that filters routes redistributed into BGP. If this option is not specified, all routes from the specified source are redistributed into BGP.
metric *metric*	Optional. Multi-Exit Discriminator (MED) metric value applied to redistributed routes. The range of values is 0 to 4,294,967,295. The default value is 0.

Default

Routes learned by other protocols are not distributed into BGP. If no metric value is specified, no MED is sent out with a redistributed route.

Usage Guidelines

Use the **redistribute** command to redistributes routes learned through other protocols and sources into the BGP routing process. More than one **redistribute** command can be specified.

The **metric** *metric* construct applies a MED attribute to redistributed routes. The MED attribute enables a peer receiving routes to select the optimal exit point (among multiple points) to a remote autonomous system. If all other factors in determining an exit point are equal, the exit point with the lowest MED metric is preferred. If a MED is received over an external BGP link, it is propagated over internal links within the autonomous system. When the update is sent on to another autonomous system, the MED attribute is stripped.

The MED value can also be set using the **metric-out** command in BGP group configuration mode and through the **set metric** command in route map configuration mode.

Use the **no** form of this command to disable the type of route redistribution specified.

Examples

The following example redistributes RIP routes into the BGP autonomous system number `321` with a metric of `1`:

```
local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#redistribute rip metric 1
```

Related Commands

metric-out
route-map—context configuration mode
set metric
show ip bgp

remove-private-AS

remove-private-AS

no remove-private-AS

Purpose

Strips the private autonomous system number (ASN) from Border Gateway Protocol (BGP) update messages sent to external peers.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

This command has no keywords of arguments.

Default

Private ASNs are included in update messages to external peers.

Usage Guidelines

Use the remove-private-AS command to strip the private ASN from BGP update messages sent to external peers. This command has no effect on internal BGP peers. The private ASN range of values, defined in RFC 1930, *Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*, is 64,512 through 65,535.

To strip the private ASN from BGP update messages sent by a group to its external peers, enter this command in BGP group configuration mode. To strip the private ASN from BGP updates sent by individual peers, enter this command in BGP peer configuration mode.

Use the **no** form of this command to return BGP to its default behavior.

Examples

The following example strips private ASNs from update messages sent by the group called `customer1` to external BGP peers:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#remove-private-as
```

The following example strips private ASNs from update messages sent by the peer at IP address `192.20.12.10` to external BGP peers:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#remove-private-as
```

Related Commands

show ip bgp

route-map

route-map *map-name* {**in** | **out**}

no route-map *map-name* {**in** | **out**}

Purpose

Applies a preconfigured route map to incoming or outgoing Border Gateway Protocol (BGP) updates.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

map-name	Name of the route map created using the **route-map** command in context configuration mode.
in	Applies the specified route map to incoming routes.
out	Applies the specified route map to outgoing routes. This option is only available in BGP group configuration mode.

Default

No route maps are applied to BGP updates.

Usage Guidelines

Use the **route-map** command to apply a route map to a BGP group or a BGP peer. Route maps are configured using the **route-map** command in context configuration mode.

Use the **in** keyword to apply the route map to incoming routes. If the route map that is specified does not exist, no routes are accepted from peers. If no import policy is specified, all routes are accepted from peers.

Use the **out** keyword to apply the route map to a BGP group's outgoing routes. You cannot apply a route map to a BGP peer's outgoing routes. All active routes from the local routing information base (RIB) that are allowed by the route map (and all other BGP policy criteria) are exported to peers. If the route map specified does not exist, no routes are exported to peers.

Use the **no** form of this command to remove the specified route map.

Examples

The following example applies the route map called `block_as_10` to outgoing routes from BGP group `customer1`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer
[local]RedBack(config-group)#route-map block_as_10 out
```

The following example applies the route map called `block_as_20` to incoming routes from the BGP peers at IP address `192.20.12.10`:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack(config-peer)#route-map block_as_20 in
```

Related Commands

route-map—context configuration mode
show ip bgp paths

router bgp

router bgp *asn* [**routing-domain** *id*]

no router bgp *asn* [**routing-domain** *id*]

Purpose

Enables the Border Gateway Protocol (BGP) routing process for the specified context.

Command Mode

context configuration

Syntax Description

asn	Autonomous system number (ASN). The range of values is 1 to 65,535.
routing-domain *id*	Optional. Local subautonomous system in the confederation. The range of values is 1 to 65,535. The default value is 0.

Default

BPG routing is not enabled.

Usage Guidelines

Use the **router bgp** command to enable the BGP routing process for the specified context. Before a BGP routing process can be enabled, you must configure a router ID using the **router-id** command in context configuration mode. Each context running BGP must be assigned a unique ASN, which is included in the open messages sent between BGP peers to establish a connection.

You can also divide an autonomous system into sub-autonomous systems grouped by a routing domain identifier. The AS and its subautonomous systems are part of the same confederation. To the outside world, the confederation looks like a single AS. Each subautonomous system is fully meshed within itself and has a few connections to other subautonomous systems in the confederation. Neighbors from other subautonomous systems are treated as special E-BGP peers. Even though peers in different subautonomous system engage in E-BGP sessions, they exchange routing information as if they were I-BGP peers. Specifically, the next-hop selection, the Multi-Exit Discriminator (MED) attribute, and the local preference is preserved, so that a single Interior Gateway Protocol (IGP) is used for all of the subautonomous systems.

To modify an ASN or routing domain identifier value, or to add a routing domain identifier to a BGP routing process, first use the **no** form of this command to remove the existing values. Then apply the **router bgp** command with the new ASN or routing domain identifier value, or both.

Use the **no** form of this command to disable BGP routing.

Examples

The following example configures a BGP routing process for autonomous system `321`:

```
[local]RedBack(config-ctx)#router bgp 321
```

The following example configures an ASN of `20` (externally-visible AS) and a routing domain identifier of `65050` (internally-visible AS) for the BGP routing process:

```
[local]RedBack(config-ctx)#router bgp 20 routing-domain 65050
```

Related Commands

router-id
show ip bgp

router-id

router-id *ip-address*

Purpose

Configures the Subscriber Management System (SMS) device identifier, which is exchanged in Border Gateway Protocol (BGP) routing messages.

Command Mode

context configuration

Syntax Description

ip-address	IP address of the SMS interface that is used as the router identifier.

Default

A router ID is not preconfigured.

Usage Guidelines

Use the **router-id** command to configure the SMS device identifier, which is exchanged in BGP routing messages. A router ID must be configured before the BGP routing process can be enabled.

Note This command is also described in Chapter 33, "OSPF Commands."

Examples

The following example configures the IP address `192.34.200.10` as the router ID:

```
[local]RedBack(config-ctx)#router-id 192.34.200.10
```

Related Commands

router bgp
show ip bgp

route-reflector-client

route-reflector-client

no route-reflector-client

Purpose

Identifies the Subscriber Management System (SMS) device as an internal Border Gateway Protocol (I-BGP) route reflector and the I-BGP peers within the group as route reflector clients.

Command Mode

BGP group configuration

Syntax Description

This command has no keywords or arguments.

Default

Peers in a group are not route reflector clients.

Usage Guidelines

Use the **route-reflector-client** command to specify the SMS device as an I-BGP route reflector and to identify peers in the BGP group as route reflector clients. This command is available only if the group is configured as an I-BGP group. An I-BGP group has the same ASN as the local ASN specified in the **router bgp** *asn* command construct.

Internal peers are divided into two groups: client peers and nonclient peers. A route reflector device reflects routes between these two groups. The route reflector and its client peers form a cluster. Nonclient peers must be fully meshed with each other. Client peers are not required to be fully meshed and do not communicate with BGP speakers outside their cluster.

When the route reflector receives an advertised route:

- Any route from an external BGP speaker is advertised to all peers.
- Any route from a nonclient peer is advertised to all client peers.
- Any route from a client peer is advertised to all peers.

If a route reflector cluster has more than one route reflector, use the **cluster-id** command to apply the same cluster ID to all route reflectors.

To disable routes learned by a client from being reflected to other clients, use the **no client-to-client** command.

Use the **no** form of this command to disable route reflector client status.

Examples

The following example configures peers in the group called `customer1` as route reflector clients:

```
[local]RedBack(config-ctx)#router bgp 321
[local]RedBack(config-bgp)#group customer1
[local]RedBack(config-group)#route-reflector-client
```

Related Commands

client-to-client
cluster-id
show ip bgp

show ip bgp

show ip bgp [*ip-address*]

Purpose

Displays entries in the Border Gateway Protocol (BGP) routing table.

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address.

Default

None

Usage Guidelines

Use the **show ip bgp** command without any arguments to list the router ID, network prefix, next-hop address, Multi-Exit Discriminator (MED) attribute, autonomous system (AS) paths, and route precedence and preference information.

Examples

The following example displays output from the **show ip bgp** command. Table 34-2 describes the fields.

```
[local]RedBack>show ip bgp
Local router ID   1.1.1.1
Status codes:   * valid, > best
Origin codes:   i - IGP, e - EGP, ? - incomplete

   Network          Next Hop     MED    Prec  Pref  LocPref  Path
*> 30.0.0.0/8       20.1.1.5     0      170   0     100      2 i
*> 40.0.0.0/8       20.1.1.5     0      170   0     100      2 i
*> 50.0.0.0/8       20.1.1.5     0      170   0     100      2 i
```

Table 34-2 show ip bgp Field Descriptions

Field	Description
Local router ID	Router ID.
Status codes	* indicates a valid table entry. > indicates the best path.
Origin codes	i indicates the entry originated from an IGP. e indicates the entry originated from an EGP. ? indicates the origin of the entry is unknown.
Network	Network address.
Next Hop	IP address of the BGP next hop.
MED	MED value.
Prec	Precedence of the route.
Pref	Preference of the route.
LocPref	Local preference of the route.
Path	List of autonomous systems that must be crossed to reach the destination.

The following is sample output from the **show ip bgp** *ip-address* command. Table 34-3 describes the fields.

```
[local]RedBack>show ip bgp 30.0.0.0
BGP routing table entry for 30.0.0.0/8
Nexthop:      20.1.1.5         Precedence:   170
Nexthop IGP:  ospf             IGP Metric    11
Peer AS:      2                Interface:    enet1
Age:          6:80             Preference:   0
MED:          0                LocalPref:    100
AS Path:      2                IGP (Id 3)
Route status: valid
```

Table 34-3 show ip bgp *prefix* Field Descriptions

Field	Description
Nexthop	IP address of the BGP next hop
Precedence	Precedence of the route
Next Hop IGP	IGP used to resolve the BGP next hop and the IGP cost to the BGP next hop
Peer AS	Number of the AS to which the peer that sent the route information belongs
Interface	Outgoing interface for the route
Age	Age of the route
Preference	Preference of the route
MED	MED value
LocalPref	Local preference of the route
AS Path	List of autonomous systems that must be crossed to reach the destination
IGP	Interior Gateway Protocol
Route status	Status of the route

Related Commands

clear ip bgp
debug ip bgp
enable-peer
group
neighbor
precedence
router bgp

show ip bgp groups

show ip bgp groups [*group-name*]

Purpose

Displays Border Gateway Protocol (BGP) group information.

Command Mode

operator exec

Syntax Description

group-name	Optional. Name of the group to be displayed.

Default

None

Usage Guidelines

Use the **show ip bgp groups** command to list BGP groups, the type (external or internal) and number of peers in a group, the autonomous system number to which a group belongs, and to view the established state of the group.

Examples

The following example provides sample output from the **show ip bgp groups** command. Table 34-4 describes the fields.

```
[local]RedBack>show ip bgp groups as2

Type       AS    Peers    Established    Name
External   2     1        1              as2
```

Table 34-4 show ip bgp groups *group-name* Field Description

Field	Description
Type	Peers in the group are either external or internal.
AS	Number of the autonomous system to which peers in the group belong.
Peers	Number of peers in the group.
Established	Number of established peers.
Name	Name of the group.

Related Commands

clear ip bgp
debug ip bgp
enable-peer
group
neighbor

show ip bgp neighbors

show ip bgp neighbors [*ip-address*] [**advertised-routes** | **received-routes** | **routes**]

Purpose

Display information about Border Gateway Protocol (BGP) neighbors.

Command Mode

operator exec

Syntax Description

ip-address	Optional. IP address of the neighbor. If this argument is omitted, all neighbors are displayed.
advertised-routes	Optional. Displays all the routes that have been advertised to the neighbor.
received-routes	Optional. Displays all the routes received from the neighbor.
routes	Optional. Displays all active routes related to the neighbor.

Default

None

Usage Guidelines

Use the **show ip bgp neighbors** command to display information about BGP peers.

Examples

The following example provides sample output of the **show ip bgp neighbors** command. Table 34-5 describes the fields.

```
[local]RedBack>show ip bgp neighbors

Peer:         20.1.1.2+13773       State:           Established
Local:        20.1.1.1+179         Type:            External
Last State:   OpenConfirm          Last Event:      RecvKeepAlive
Last Error:   None                 Peer Version:    4
Route Queue:  empty                Active Holdtime: 180
Last Ex:      41                   Last Tx:         24
Total Msg Rx: 3280                 Updates Rx:      1
```

Table 34-5 show ip bgp neighbors Field Description

Field	Description
Peer	IP address of the peer plus the peer's TCP port number
State	Internal state of the BGP connection
Local	IP address of the local BGP system plus the local TCP port number
Type	Peer type—either external or internal
Last State	Previous state of the BGP connection
Last Error	Last error that occurred on the BGP connection
Peer Version	BGP version that the peer is running
Route Queue	Number of outgoing routes queued for the peer
Active Holdtime	Maximum interval that the local BGP system waits between update messages from the peer before terminating the BGP session
Last Rx	Time that has elapsed since the local system received BGP messages from the peer
Last Tx	Time that has elapsed since the local system sent BGP messages to the peer
Total Msg Rx	Total number of BGP messages received from the peer
Updates Rx	Total number of BGP update messages received from the peer

The following example provides sample output from the **show ip bgp neighbors** *ip-address* **routes** command. Table 34-6 describes the fields.

```
[local]RedBack>show ip bgp neighbors 20.1.1.2 routes

Local router ID 1.1.1.1
Status codes: * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop     Metric     Prec    Path
*> 30.0.0.0/8       20.1.1.5     0          170     2 i
*> 40.0.0.0/8       20.1.1.5     0          170     2 i
*> 50.0.0.0/8       20.1.1.5     0          170     2 i
```

Table 34-6 show ip bgp neighbors *ip_address* routes Field Description

Field	Description
Local router ID	Router ID or IP address.
Status codes	* indicates a valid table entry. > indicates the best path.
Origin codes	i indicates the entry originated from an IGP. e indicates the entry originated from an EGP. ? indicates the origin of the entry is unknown.
Network	Network address.
Next Hop	IP address of the next system that will be used when forwarding a packet to its destination.
Metric	Multi-Exit Discriminator (MED) value.
Prec	Precedence of the route.
Path	List of autonomous systems that must be crossed to reach the destination.

Related Commands

accept-med
always-compare-med
debug ip bgp
enable-peer
metric-out
neighbor
router bgp
router-id

show ip bgp paths

show ip bgp paths

Purpose

Displays all Border Gateway Protocol (BGP) autonomous system (AS) paths in the database.

Command Mode

operator exec

Syntax Description

The **show ip bgp** command has several keyword constructs. Each construct each treated as a separate command. See the “Related Commands” section for a list of all **show ip bgp** commands.

Default

None

Usage Guidelines

Use the **show ip bgp paths** command to list all AS path information.

Examples

The following example provides sample output from the **show ip bgp paths** command. Table 34-7 describes the fields.

```
[local]RedBack>show ip bgp paths

Hash     Id     Refs    Path
96       1      3       i<Atomic,Local>
0        2      16      i
0        3      5      (1) 2 i
```

Table 34-7 show ip bgp paths

Field	Description
Hash	Hashed key value of the path.
Id	Internally assigned ID for the AS path.
Refs	Number of routes that share this AS path.
Path	Path content.

Related Commands

debug ip bgp
remove-private-AS
router bgp

show ip bgp summary

show ip bgp summary

Purpose

Displays status of all Border Gateway Protocol (BGP) sessions.

Command Mode

operator exec

Syntax Description

The **show ip bgp** command has several keyword constructs. Each construct each treated as a separate command. See the “Related Commands” section for a list of all **show ip bgp** commands.

Default

None

Usage Guidelines

Use the **show ip bgp summary** command to display information on BGP sessions.

Examples

The following example provides sample output from the **show ip bgp summary** command. Table 34-8 describes the fields.

```
[local]RedBack>show ip bgp summary

1 bgp peers, 0 established peer, 1 peer groups
16 network entries, 3 BGP path attribute entries

Neighbor      Ver   AS   RxPfx   TxPfx      Up/Down    State
20.1.1.1      4     2    0       0          5:56       Active
```

Table 34-8 show ip bgp summary

Field	Description
Neighbor	IP address of the neighbor
Ver	BGP version spoken to the neighbor
AS	Number of the autonomous system to which the neighbor belongs
RxPfx	Number of network prefixes received from the neighbor
TxPfx	Number of network prefixes sent to the neighbor
Up/Down	Time elapsed (dd:hh:mm:ss) since last transition in or out of the established state
State	Current state of the BGP session

Related Commands

debug ip bgp
enable-peer
router bgp
show ip bgp
show ip bgp groups
show ip bgp neighbors
show ip bgp paths

throttle

throttle *rate*

no throttle

Purpose

Sets the rate at which Border Gateway Protocol (BGP) update messages are sent to peers.

Command Mode

BGP group configuration

Syntax Description

rate	Number of updates sent per second. The range of values is 1 to 65,535.

Default

No rate control is performed on BGP update messages.

Usage Guidelines

Use the **throttle** command to send no more than the specified number of BGP update messages per second to peers.

Use the **no** form of this command to remove BGP update message rate control.

Examples

The following example configures the maximum number of BGP updates that are sent to peers is to 5 per second:

```
[local]RedBack(config-group)#throttle 5
```

Related Commands

enable-peer
neighbor
show ip bgp neighbors

ttl

ttl *seconds*

no ttl

Purpose

Sets the time to live (TTL) value for IP packets containing Border Gateway Protocol (BGP) messages when communicating with peers.

Command Mode

BGP group configuration
BGP peer configuration

Syntax Description

seconds	TTL in seconds. The range of values is 1 through 255.

Default

The TTL for external peers is 1. For multihop external peers, or for internal peers, the TTL is 255.

Usage Guidelines

Use the **ttl** command to change the TTL value used communicating with BGP peers.

To apply the TTL value to a group, enter this command in BGP group configuration mode. To apply the TTL value to a peer, use this command in BGP peer configuration mode.

Use the **no** form of this command to return the TTL to its default value.

Examples

The following example sets the TTL for the group called `customer` to `10`:

```
[local]RedBack(config-bgp)#group customer
[local]RedBack#(config-group)#ttl 10
```

The following example sets the TTL for the peer at IP address `192.20.12.10` to `10`:

```
[local]RedBack(config-group)#neighbor 192.20.12.10
[local]RedBack#(config-group)#ttl 10
```

Related Commands

show ip bgp neighbors

Chapter 35

Routing Policy Commands

This chapter describes the commands used to configure and maintain routing policies supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure routing policies, and configuration examples, see the "Configuring Routing Policies" chapter in the *Access Operating System (AOS) Configuration Guide*.

as-path access-list

as-path access-list *list-num* **seq** *seq-num* {**deny** | **permit**} *as-reg-exp*

no as-path access-list *list-num* **seq** *seq-num* {**deny** | **permit**} *as-reg-exp*

Purpose

Configures a Border Gateway Protocol (BGP) autonomous system (AS) path access control list.

Command Mode

context configuration

Syntax Description

list-num	Decimal value representing the regular expression access list number. The range of values is 1 to 199.
seq *seq-num*	Specifies the sequence number in a range from 1 to 65,535, indicating the position this AS path access list will have with respect to other AS path access lists with the same access list number. The AS path access list with the lowest sequence number is looked at first by the system.
deny	Causes any route matching the criteria to be dropped.
permit	Causes any route matching the criteria to be accepted.
as-reg-exp	Regular expression of AS paths. See the “Usage Guidelines” section for details.

Default

There are no preconfigured AS path access control lists.

Usage Guidelines

Use the **as-path access-list** command to configure a BGP AS path access control list. You can specify an access list filter on both inbound and outbound BGP routes. Each filter is an access list based on regular expressions. If the regular expression matches the representation of the AS path of the route as a set of AS numbers (ASNs), the **permit** or **deny** condition applies. The AS path does not contain the local ASN. Apply the AS path access list to a route map using the **match as-path** command. Apply the route map as appropriate.

Use the **no** form of this command to remove or modify an AS path access list.

A regular expression (regex) can contain the following:

- *term*
- *regex1 regex2* (an AS path that matches both regular expression 1 *and* 2)
- *regex1* | *regex2* (an AS path that matches either regular expression 1 *or* 2)

The *term* argument can be one of the following variables:

- *asn*

  Matches the provided ASN. The ASN is a positive 16-bit number. The ASN range is 0 to 65,534.

- !*asn*

  Matches any ASN except for the one provided.

- *asn1 - asn2*

  Matches the specified range of ASNs.

- !*asn1 - asn2*

  Matches the range of ASNs except those in the range from *asn1* to *asn2*.

- .

  Matches any ASN.

- **null**

  Matches an empty string.

- [*as-range-list*]

  Brackets define a set of autonomous systems, one of which must be matched. An item in this list can be either a single autonomous system or a range of autonomous systems.

  For example, [*asn1 asn2–asn3 asn4*] is equivalent to (*asn1* | *asn2–asn3* | *asn4*).

- (*regex*)

  Parentheses act to group expressions to make a *term* out of any regular expression. An operator, such as * or ?, works on a regular expression enclosed in parentheses as it would on any *term*.

- *term* (*m*, *n*)

  A term followed by *m*, *n* where *m* and *n* are non-negative integers, *m*<=*n* means at least *m* and at most *n* repetitions of *term*.

- *term* (*m*)

  A *term* followed by *m*, where *m* is a positive integer, matches exactly *m* repetitions of *term*.

- *term* (*m*,)

  A *term* followed by *m*, where *m* is a positive integer, matches *m* or more repetitions of *term*.

- *term* *****

  A *term* followed by * matches zero or more repetitions of *term*. This is shorthand for {0,}.

- *term* **+**

  A *term* followed by + matches one or more repetitions of *term*. This is shorthand for {1,}.

Normally the command-line interface interprets ? as a help command. To bypass this default behavior when using regular expressions, type the key sequence Ctrl+v followed by ?.

Spaces are ignored except when specifying more than one AS number in a series.

The following list provides examples and descriptions of regular expressions:

- **.* 1**

  Indicates any path that originates ins ASN 1. For example, a match could be 1 or 2 1 or 5 4 3 2 1.

- **1+**

  Indicates any path that consists of one or more occurrences of ASN 1. For example, a match could be 1 or 1 1 1.

- **1**

  Indicates that ASN 1 must be the path. A match could only be 1.

- **.1|2.* or .(1|2).***

  Indicates any path with a second ASN or 1 or 2. For example, a match could be 1 1 or 1 2 3 or 10 1 100 or 3 2.

- **[1-3 10]?**

  Indicates paths 1 or 2 or 3 or 10 or null. A match could be 1 or 2 or 3 or 10 or null.

- **.* 1!**

  Indicates all paths that do not originate in ASN 1. For example, a match could be 1 2 or 2 3 5.

Examples

The following example configures the BGP neighbor at IP address `10.1.1.1` not to send advertisements about any path through or from the adjacent autonomous system `3`:

```
[local]RedBack(config-ctx)#as-path access-list 10 seq 5 deny .*3.*
[local]RedBack(config-ctx)#as-path access-list 10 seq 10 permit .*
[local]RedBack(config-ctx)#route-map drop-asp-3 permit 10
[local]RedBack(config-route-map)#match as-path 10
.
.
.
[local]RedBack(config-ctx)#router bgp 65015
[local]RedBack(config-bgp)#group as65012 remote-as 65012
[local]RedBack(config-group)#neighbor 10.1.1.1
[local]RedBack(config-peer)#route-map drop-asp-3 out
[local]RedBack(config-peer)#enable-peer
```

Related Commands

match as-path
show as-path-access-list

community-list

community-list *list-num* **seq** *seq-num* {**deny** | **permit**} {*community-num* | **internet** | **local-AS** | **no-advertise | no-export**}

no community-list *list-num* **seq** *seq-num*

Purpose

Configures a Border Gateway Protocol (BGP) community list.

Command Mode

context configuration

Syntax Description

list-num	Decimal value. The range of values is 1 to 99.
seq *seq-num*	Sequence number. The range of values is 1 to 65,535. The sequence number indicates the position this community list has with respect to other community lists with the same *list-num* value. The community list with the lowest sequence number is looked at first by the system.
deny	Causes any route matching the criteria to be dropped.
permit	Causes any route matching the criteria to be accepted.
community-num	Unsigned decimal or encoded 32-bit value. The range of unsigned decimal values is 1 to 4,294,967,295. The encoded 32-bit value must be in aa:nn format, where aa is the autonomous system number (ASN) and nn is a 2-byte number. You can specify a single number or multiple numbers separated by a space. (All numbers must match a community in the route being tested in order for the statement to match.)
internet	Specifies the Internet community; that is, it matches any community.
local-AS	Propagates this route only to peers in the local autonomous system (AS). Does not send this route to external peers even if they are in the same confederation.
no-advertise	Does not advertise this route to any peer (internal or external).
no-export	Does not advertise this route out of the local AS confederation, or out of the local AS, if it is not part of a confederation.

Default

There are no preconfigured community lists.

Usage Guidelines

Use the **community-list** command to configure a Border Gateway Protocol (BGP) community list. A community is a group of destinations that share some common attributes. Each destination can belong to multiple communities. You can filter routes based on community information. Choose an individual community number or a common community number specified by any of these keywords: **internet**, **local-AS**, **no-advertise**, or **no-export**. You can enter a series of community numbers. Like access control lists, you can configure a series of community lists. Statements are checked until a match is found.

To set the communities attribute and match clauses based on communities, use the **set community** and **match community-list** commands in route map configuration mode.

To use the *community-num* argument, you must first enable the **ip bgp-community** command before the 32-bit value format is accepted.

Use the **no** form of this command to remove a community list or modify a community list's settings.

Examples

The following example configures community list number `1` to propagate routes to peers within the local autonomous system (`local-AS`):

```
[local]RedBack(config-ctx)#community-list 1 seq 10 permit local-AS
```

Related Commands

ip bgp-community
match community-list
set community
show community-list

ip bgp-community

ip bgp-community new-format

no ip bgp-community new-format

Purpose

Configures the system to display Border Gateway Protocol (BGP) communities in autonomous system number (ASN) 2-byte number format.

Command Mode

context configuration

Syntax Description

new-format	Selects the *aa:nn* format where *aa* is the ASN and *nn* is a 2-byte number.

Default

Community lists use unsigned decimal values for community list number.

Usage Guidelines

Use the **ip bgp-community new-format** command to configure the system to display BGP communities in ASN/2-byte number format. Use this command in conjunction with the **community-list** command. When the **ip bgp-community** command is enabled, the *community-num* argument for the **community-list** command can be entered in *aa:nn* format instead of in unsigned decimal format. With the new format, the first two octets (*aa*) provide an ASN. The final two octets (*nn*) are defined by the autonomous system.

Use the **no** form of this to command return the display of community numbers to unsigned decimal format.

Examples

The following example enables the display of BGP communities in *aa:nn* format:

```
[local]RedBack#(config-ctx)#ip bgp-community new-format
```

Related Commands

community-list

match as-path

match as-path *list-num* [*...list-num*]

no match as-path *list-num* [*...list-num*]

Purpose

Matches a Border Gateway Protocol (BGP) autonomous system (AS) path access control list.

Command Mode

route map configuration

Syntax Description

list-num	Integer that represents the AS path access control list. The range of values is 1 to 199.

Default

There are no preconfigured AS path lists.

Usage Guidelines

Use the **match as-path** command to match a BGP AS path access control list. A route map can have several parts. Any route that does not match at least one **match** clause corresponding to a route map is ignored. That is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit **match** specified.

Examples

The following example sets the autonomous system path to match BGP autonomous system path access control list 5:

```
[local]RedBack(config-ctx)#route-map asp-regex permit 10
[local]RedBack(config-route-map)#match as-path 5
```

Related Commands

as-path access-list
route-map—context configuration mode
show route-map

match community-list

match community-list *list-num* [*...list-num*]

no match community-list *list-num* [*...list-num*]

Purpose

Distributes routes with a matching Border Gateway Protocol (BGP) community list.

Command Mode

route map configuration

Syntax Description

list-num	Decimal value. The range of values is 1 to 99.

Default

There are no preconfigured community lists.

Usage Guidelines

Use the **match community-list** command to distribute routes with a matching BGP community list. A community is a group of destinations that share some common attributes. Each destination can belong to multiple communities. To create a community list, use the **community-list** command in context configuration mode. Statements are checked until a match is found.

Use the **no** form of this command to disable the configured match condition.

Examples

The following example distributes any route that has the community `11` attribute:

```
[local]RedBack(config-ctx)#community-list 1 permit 11
[local]RedBack(config-ctx)#route-map map_A
[local]RedBack(config-route-map)#match community-list 1
```

Related Commands

community-list
route-map—context configuration mode
set community
show route-map

match interface

match interface *if-name* [*...if-name*]

no match interface *if-name* [*...if-name*]

Purpose

Distributes routes that connect to a next hop IP address through the interface.

Command Mode

route map configuration

Syntax Description

if-name	Name of the interface that must be matched.

Default

There is no preconfigured match interface.

Usage Guidelines

Use the **match interface** command to distribute routes that connect to a next-hop IP address through the interface.

Use the **no** form of this command to disable the configured match condition.

Examples

The following example distributes routes with a next hop of interface `ether0`:

```
[local]RedBack(config-ctx)#route-map rmap_A
[local]RedBack(config-route-map)#match interface ether0
```

Related Commands

interface
route-map—context configuration mode
show route-map

match ip address

match ip address *list-num* [*...list-num*]

no match ip address *list-num* [*...list-num*]

Purpose

Distributes routes that have a destination IP address permitted by the specified route access control lists.

Command Mode

route map configuration

Syntax Description

list-num	Number (an integer) of the route access control list. The range of values is 1 to 99.

Default

There are no preconfigured route access list numbers.

Usage Guidelines

Use the **match ip address** command to distribute routes with a destination IP address permitted by the specified route access control list or lists. To create a route access control list, use the **route-access-list** command in context configuration mode.

Use the **no** form of this *c*ommand to disable the configured match condition.

Examples

The following example distributes routes that have destination IP addresses specified in either route access list 5 or 88:

```
[local]RedBack(config-ctx)#route-map rmap_B
[local]RedBack(config-route-map)#match ip address 5 88
```

Related Commands

route-access-list standard-access-list-num
route-map—context configuration mode
show route-map

match ip next-hop

match ip next-hop *list-num* [*...list-num*

no match ip next-hop *list-num* [*...list-num*]

Purpose

Distributes routes with a next-hop IP address that is permitted by the specified route access control list or lists.

Command Mode

route map configuration

Syntax Description

list-num	Integer. The range of values is 1 to 99.

Default

Routes are routed without being required to match a next-hop IP address.

Usage Guidelines

Use the **match ip next-hop** command to distribute routes with a next-hop IP address permitted by the specified route access list or lists. To create a route access list, use the **route-access-list** command in context configuration mode.

Use the **no** form of this command to disable the configured match condition.

Examples

The following example distributes routes which include a next-hop IP address permitted by either route access control list `11` or `88`:

```
[local]RedBack(config-ctx)#route-map rmap_C
[local]RedBack(config-route-map)#match ip next-hop 11 88
```

Related Commands

route-access-list standard-access-list-num
route-map—context configuration mode
set ip next-hop
show route-map

match metric

match metric *metric*

no match metric *metric*

Purpose

Distributes routes with a matching metric value.

Command Mode

route map configuration

Syntax Description

metric	Route metric. The range of values is 0 to 4,294,967,295.

Default

Routes are distributed without being required to match a metric value.

Usage Guidelines

Use the **match metric** command to distribute routes that match a configured metric value.

Use the **no** form of this command to disable the configured match condition.

Examples

The following example distributes routes with a metric value of 5:

```
[local]RedBack(config-ctx)#route-map rmap_D
[local]RedBack(config-route-map)#match metric 5
```

Related Commands

route-map—context configuration mode
set metric
show route-map

match route-type

match route-type {**local** | **internal** | **external** [**type-1** | **type-2**]}

no match route-type {**local** | **internal** | **external** [**type-1** | **type-2**]}

Purpose

Distributes routes that match the type specified: local, internal, or external (types 1 and 2).

Command Mode

route map configuration

Syntax Description

local	Distributes locally generated Border Gateway Protocol (BGP) routes.
internal	Distributes internal Open Shortest Path First (OSPF) intraarea and interarea routes.
external	Specifies OSPF external routes.
type-1	Distributes OSPF type 1 external routes.
type-2	Distributes OSPF type 2 external routes.

Default

Routes are distributed without being required to match route types.

Usage Guidelines

Use the **match route-type** command to distribute routes matching a specific route type.

Use the **no** form of this command to disable the configured match condition.

Examples

The following example distributes internal OSPF routes:

```
[local]RedBack(config-ctx)#route-map map_E
[local]RedBack(config-route-map)#match route-type internal
```

Related Commands

route-map—context configuration mode
show route-map

match tag

match tag *tag*

no match tag

Purpose

Distributes routes that match the specified tag value.

Command Mode

route map configuration

Syntax Description

tag	Unsigned integer. The range of values is 0 to 4,294,967,295.

Default

There are no preconfigured tag values.

Usage Guidelines

Use the **match tag** command to distribute routes with a matching tag value.

Use the **no** form of this command to disable the configured match condition.

Examples

The following example distributes routes with a tag of 5:

```
[local]RedBack(config-ctx)#route-map map_F
[local]RedBack(config-route-map)#match tag 5
```

Related Commands

route-map—context configuration mode
show route-map

route-access-list *extended-access-list-num*

route-access-list *extended-access-list-num* **seq** *seq-num* {**deny** | **permit**} {*ip-address* | **any**} [*wildcard*] [*netmask* | **any**] [*netmask wildcard*]

no route-access-list *extended-access-list-num* [**seq** *seq-num*]

Purpose

Creates an extended route access control list that allows filtering on any set of prefix lengths combined with any set of network numbers.

Command Mode

context configuration

Syntax Description

extended-access-list-num	Extended access control list number (a decimal). The range of values is 100 to 199.
seq *seq-num*	Sequence-number. The range of values is 1 to 65,535. The sequence number indicates the position this route access list has with respect to other route access lists with the same access list number. The route access list with the lowest sequence number is looked at first by the system.
deny	Causes any route matching the criteria to be dropped.
permit	Causes any route matching the criteria to be accepted.
ip-address	Network address to be included in the permit or deny criteria.
any	Signifies that any IP address will be included in the permit or deny criteria.
wildcard	Optional. Indication of which bits in the specified IP address are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *wildcard* argument mean that the corresponding bits in the *ip-address* argument must match; one-bits in the *wildcard* argument mean that the corresponding bits in the *ip-address* argument are ignored.
netmask	Network mask to be combined with *ip-address* in the form A.B.C.D.
any	An abbreviation for a *netmask* and *netmask wildcard* of 0.0.0.0 255.255.255.255.

netmask wildcard	Network mask wildcard. Identifies which bits in the specified *netmask* are significant for the purpose of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the wildcard mean that the corresponding bits in the *netmask* argument must match. One-bits in the wildcard mean that the corresponding bits in the *netmask* argument are ignored.

Default

There are no preconfigured route access lists.

Usage Guidelines

Use the **route-access-list** *extended-access-list-num* command to configure an extended route access control list that allows filtering on any set of prefix lengths combined with any set of network numbers. Use this command in conjunction with the **match ip address** command in route map configuration mode, which specifies the access list number that must be matched for the route to be allowed or denied redistribution.

Use the **no** form of this command to delete a specific route entry if the *seq-num* argument is specified. If only the *access-list-num* argument is specified, the entire route access list is deleted.

Examples

The following example permits routes in the network address range `81.1.0.0 255.255.0.0`, but denies any more-specific routes of `81.1.0.0` (including `81.1.0.0 255.255.255.0`):

```
[local]RedBack(config-ctx)#route-access-list 101 seq 10 permit 81.1.0.0 0.0.0.0
255.255.0.0 0.0.0.0
[local]RedBack(config-ctx)#route-access-list 101 seq 20 deny 81.1.0.0 0.0.255.255
255.255.0.0 0.0.255.255
```

Related Commands

match ip address
route-map

route-access-list *standard-access-list-num*

route-access-list *standard-access-list-num* **seq** *seq-num* {**deny** | **permit**} {*ip-address* | **any**} [*wildcard*]

no route-access-list *standard-access-list-num* [**seq** *seq-num*]

Purpose

Configures a standard route access control list that allows or prevents the acceptance of routes from specified sources, or the advertisement of routes to specified destinations.

Command Mode

context configuration

Syntax Description

standard-access-list-num	Standard access control list number (a decimal). The range of values is 1 to 99.
seq *seq-num*	Specifies the sequence number. The range of values is 1 to 65,535. The sequence number indicates the position this route access control list has with respect to other route access lists with the same access control list number. The route access control list with the lowest sequence number is looked at first by the system.
deny	Causes any route matching the criteria to be dropped.
permit	Causes any route matching the criteria to be accepted.
ip-address	Network address to be included in the permit or deny criteria.
any	Signifies that any IP address is included in the permit or deny criteria.
wildcard	Optional. An indication of which bits in the specified IP address are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *wildcard* argument mean that the corresponding bits in the *ip-address* argument must match; one-bits in the *wildcard* argument mean that the corresponding bits in the *ip-address* argument are ignored

Default

There are no preconfigured route access control lists.

Usage Guidelines

Use the **route-access-list** *standard-access-list-num* to configure a standard route access control list that allows or prevents the acceptance of routes from specified sources, or the advertisement of routes to specified destinations. Use this command in conjunction with the **match ip address** command in route map configuration mode, which specifies the access list number that must be matched for the route to be allowed or denied redistribution.

Use the **no** form of this command to delete a specific route entry if the *seq-num* is specified. If only the *standard-access-list-num* argument is specified, the entire route access control list is deleted.

Examples

The following example redistributes static routes passing the **route-access-list 7** command criteria into the BGP routing process. Routes are redistributed with a metric of 10.

```
[local]RedBack(config-ctx)#route-access-list 7 seq 10 permit 81.1.0.0 0.0.255.255
[local]RedBack(config-ctx)#route-access-list 7 seq 15 permit 77.0.0.0 0.255.255.255
[local]RedBack(config-ctx)#route-map rmap1 permit 10
[local]RedBack(config-route-map)#match ip address 7
[local]RedBack(config-route-map)#set metric 10
.
.
.
[local]RedBack(config-ctx)#router bgp 65012
[local]RedBack(config-bgp)#redistribute static route-map rmap1
```

Related Commands

match ip address
route-map

route-map

route-map *map-name* [**deny** | **permit**] [*seq-num*]

no route-map *map-name* [**deny** | **permit**] [*seq-num*]

Purpose

Creates a route map for policy routing and enters route map configuration mode.

Command Mode

context configuration

Syntax Description

map-name	Descriptive name for the route map.
deny	Prevents routes from being distributed.
permit	Allows routes to be distributed.
seq-num	Sequence number. The range of values is 1 to 65,535. The default value is 10. The sequence number indicates the position this route map has with respect to other route maps with the same name. The route map with the lowest sequence number is looked at first by the system.

Default

If not specified, the action is permit. If not specified, the sequence number is 10.

Usage Guidelines

Use the **route-map** command to have detailed control over which incoming and outgoing routes will be permitted or denied with regard to particular autonomous systems. If the criteria set by the **match** command in route map configuration mode is met and the **deny** keyword is specified, the route is not distributed. No further route map sequences that share the same *map-name* argument is examined.

If the criteria set by the **match** command in route-map configuration mode is met for this route map, and **permit** is specified, the route is distributed according to the criteria specified by the **set** command in route map configuration mode. If the match criteria are not met and **permit** is specified, the next route map sequence with the same *map-name* argument is tested. If a route passes none of the match criteria for a set of route map sequences that share the same *map-name* argument, it is not redistributed.

Use the **route-map** command in conjunction with the **match** and **set** commands in route map configuration mode to specify the conditions under which redistribution is allowed for the named route map, and to dictate the actions to perform if the conditions are met. There must be at least one match statement associated with a route map.

Any route that does not match at least one condition specified by a **match** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. To modify only a subset of criteria, configure a second set of conditions for the named route map.

You can apply a particular route map to a BGP group or peer by using the **route-map** command in BGP group or BGP peer configuration mode. However, only incoming routes can be applied at the BGP peer level. You can also apply route maps to routes that are redistributed into the BGP routing process by using the **route-map** keyword with the **redistribute** command found in BGP configuration mode.

Use the **no** form of this command to delete a specific route entry if the *seq-num* argument is specified. If only the *map-name* argument is specified, the entire route map is deleted.

Examples

The following example redistributes static routes that pass the **route-access-list** command criteria into the BGP routing process. Routes are redistributed into BGP with a metric of `10`.

```
[local]RedBack(config-ctx)#route-access-list 7 seq 10 permit 81.1.0.0 0.0.255.255
[local]RedBack(config-ctx)#route-access-list 7 seq 15 permit 77.0.0.0 0.255.255.255
[local]RedBack(config-ctx)#route-map rmap1 permit 10
[local]RedBack(config-route-map)#match ip address 7
[local]RedBack(config-route-map)#set metric 10
[local]RedBack(config-route-map)#exit
[local]RedBack(config-ctx)#router bgp 65012
[local]RedBack(config-bgp)#redistribute static route-map rmap1
```

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match metric
match route-type
match tag
redistribute—BGP configuration mode
route-access-list standard-access-list-num
route-map
set as-path prepend
set community
set ip next-hop
set local-preference
set metric
set origin
set preference
show route-map

set as-path prepend

set as-path prepend *asn*

no set as-path prepend

Purpose

Prepends an autonomous system (AS) path to Border Gateway Protocol (BGP) routes passing the route map conditions.

Command Mode

route map configuration

Syntax Description

asn	Autonomous system number (ASN). Prepends the ASN to the AS path of the route matched by the route map. The range of values is 1 to 65,535. Applies to inbound and outbound BGP route maps.

Default

There is no preconfigured AS path string.

Usage Guidelines

Use the **set as-path** command to prepend an AS path to BGP routes passing the route map conditions. The only global BGP metric available to influence the best path selection is the AS path length. By varying the length of the AS path, a BGP peer can influence the best path selection. Usually the local AS number is prepended multiple times, increasing the AS path length.

Use the **no** form of this command to disable the configured set action.

Examples

The following example prepends ASN `11` to all the routes advertised to `10.1.1.1`:

```
[local]RedBack(config-ctx)#router bgp 11
[local]RedBack(config-bgp)#group test-as remote-as 12
[local]RedBack(config-group)#neighbor 10.1.1.1
[local]RedBack(config-peer)#route-map set-as-path out
.
.
.
```

```
[local]RedBack(config-ctx)#route-map set-as-path
[local]RedBack(config-route-map)#match as-path 1
[local]RedBack(config-route-map)#set as-path prepend 11 11
```

Related Commands

match as-path
route-map—context configuration mode
show route-map

set community

set community {*community-num* | **local-as** | **no-export** | **no-advertise** | **none**} [**additive**]

no set community

Purpose

Sets the Border Gateway Protocol (BGP) community attribute for routes passing the route map conditions.

Command Mode

route map configuration

Syntax Description

community-num	Unsigned decimal or encoded 32-bit value. The range of unsigned decimal values is 1 to 4,294,967,295. The encoded 32-bit value must be in aa:nn format, where aa is the autonomous system number (ASN) and nn is a 2-byte number.
local-as	Propagates this route only to peers in the local autonomous system. Does not send this route to external peers even if they are in the same confederation.
no-advertise	Does not advertise this route to any peer (internal or external).
no-export	Does not advertise this route out of the local AS confederation, or out of the local AS, if it is not part of a confederation.
additive	Optional. Adds the community to existing communities.
none	Removes the community attribute from the prefixes that pass the route map conditions.

Default

There are no preconfigured BGP communities.

Usage Guidelines

Use the **set community** command to set the BGP community attribute for routes passing the route map conditions. A community is a group of destinations that share some common attributes. Each destination can belong to multiple communities. To create a community list, use the **community-list** command in context configuration mode. Like access control lists, you can configure a series of community lists. Statements are checked until a match is found.

Use the **no** form of this command to disable the configured set action.

Examples

The following example sets the community attribute to 9 for routes that pass the autonomous system (AS) path 1 conditions. Routes that pass the AS path list 2 conditions have their community attribute set to no-export (these routes are not advertised to any BGP peer):

```
[local]RedBack(config-ctx)#route-map set_community 10 permit
[local]RedBack(config-route-map)#match as-path 1
[local]RedBack(config-route-map)#set community 9
.
.
.
[local]RedBack(config-ctx)#route-map set_community 20 permit
[local]RedBack(config-route-map)#match as-path 2
[local]RedBack(config-route-map)#set community no-export
```

Related Commands

community-list
match community-list
route-map—context configuration mode
show route-map

set ip next-hop

set ip next-hop *ip-address* [*...ip-address*] | **peer-address**]

no set ip next-hop *ip-address* [*...ip-address*] | **peer-address**]

Purpose

Determines the next-hop IP address use to forward packets for routes passing the route map conditions.

Command Mode

route map configuration

Syntax Description

ip-address	Next-hop IP address, or optionally, series of IP addresses.
peer-address	Optional. Sets the next-hop address to a Border Gateway Protocol (BGP) peer address. For an inbound route map, the system uses the IP address of the BGP neighbor's peer. For an outbound route map, the system uses the IP address of the local BGP peer.

Default

Disabled.

Usage Guidelines

Use the **set ip next-hop** command to set the next-hop IP address that is used to forward packets for routes passing the route map conditions. If the first IP address that is specified is unreachable, the next specified IP address is tried. If the **peer-address** keyword is applied to an inbound route map, the next hop of received matching routes is set to the IP address of the BGP neighbor's peer, overriding any third-party next hops. If the **peer-address** keyword is applied to an outbound route map, the next hop of the advertised matching routes is set to the IP address of the local BGP speaker, thus disabling the next-hop calculation.

Use the **no** form of this command to disable the configured set action.

Examples

The following example sets the next-hop for routes passing `route-access-list 1` to the BGP neighbor's peer IP address:

```
[local]RedBack(config-ctx)#route-map rmap_Q permit 10
[local]RedBack(config-route-map)#match route-access-list 1
[local]RedBack(config-route-map)#set ip next-hop peer-address
```

Related Commands

match ip next-hop
route-map—context configuration mode
show route-map

set local-preference

set local-preference *local-pref*

no set local-preference

Purpose

Sets the degree of preference for the Border Gateway Protocol (BGP) autonomous system (AS) path.

Command Mode

route map configuration

Syntax Description

local-pref	Integer. The range of values is 0 to 4,294,967,295.

Default

The preference value is 100.

Usage Guidelines

Use the **set local-preference** command to set the degree of preference for the AS path for routes passing the route map conditions. The preference is sent only to routers in the local autonomous system. A route with a high value is preferred over a route with a lower value.

Use the **no** form of this command to disable the configured set action.

Examples

The following example sets the local preference for all routes included in route access list `1` to `50`:

```
[local]RedBack(config-ctx)#route-map rmap_P
[local]RedBack(config-route-map)#match route-access-list 1
[local]RedBack(config-route-map)#set local-preference 50
```

Related Commands

route-map—context configuration mode
show route-map

set metric

set metric [**+** | **-**] *metric*

no set metric

Purpose

Sets the metric value for the destination routing protocol for routes passing the route map condition.

Command Mode

route map configuration

Syntax Description

+ | **-**	Optional. Adds or subtracts the metric value specified.
metric	Metric value (an integer). The range of values is 0 to 4,294,967,295.

Default

The metric value is established dynamically.

Usage Guidelines

Use the **set metric** command to set the metric value for the destination routing protocol for routes passing the route map condition.

Use the **no** form of this command to disable the configured set action.

Examples

The following example sets the metric value for the routing protocol to `50`:

```
[local]RedBack(config-ctx)#route-map rmap_M
[local]RedBack(config-route-map)#set metric 50
```

The following example adds `11` to the metric value for the routing protocol:

```
[local]RedBack(config-ctx)#route-map add_metric permit 20
[local]RedBack(config-route-map)#set metric +11
```

Related Commands

metric-out
match metric
redistribute—BGP configuration mode
route-map—context configuration mode
show route-map

set origin

set origin {**egp** | **igp** | **incomplete**}

no set origin

Purpose

Sets origin of the Border Gateway Protocol (BGP) path information for routes passing the route map condition.

Command Mode

route map configuration

Syntax Description

egp	Indicates that the path information originated from another autonomous system.
igp	Sets the origin to the local Interior Gateway Protocol (IGP).
incomplete	Indicates that the origin is unknown.

Default

The origin is determined by the route in the main IP routing table.

Usage Guidelines

Use the **set origin** command to set the BGP origin code for routes passing the route map conditions.

Use the **no** form of this command to disable the configured set action.

Examples

The following example sets the origin of routes that pass the route map conditions to IGP:

```
[local]RedBack(config-ctx)#route-map rmap_H
[local]RedBack(config-route-map)#match route-access-list 10
[local]RedBack(config-route-map)#set origin igp
```

Related Commands

route-map—context configuration mode
show route-map

set preference

set preference *pref*

no set preference

Purpose

Sets the degree of preference for Border Gateway Protocol (BGP) routes.

Command Mode

route map configuration

Syntax Description

pref	Preference value (an integer). The range of values is 0 to 65,535.

Default

Any preference value already set is not changed by the specified route map.

Usage Guidelines

Use the **set preference** command to set the degree of preference for BGP routes that pass the route map conditions. A route with a low value is preferred over a route with a higher value. The value assigned with the **set preference** command overrides the value assigned using the **preference** command in BGP group and BGP peer configuration modes.

Use the **no** form of this command to disable the configured set action.

Examples

The following example sets the BGP preference to `50` for routes that are permitted by route access list `10`:

```
[local]RedBack(config-ctx)#route-map rmap_G
[local]RedBack(config-route-map)#match route-access-list 10
[local]RedBack(config-route-map)#set preference 50
```

Related Commands

preference—BGP group and BGP peer configuration modes
route-map—context configuration mode
show route-map

show as-path-access-list

show as-path-access-list [*list-num*]

Purpose

Displays configured Border Gateway Protocol (BGP) autonomous system (AS) path access control lists.

Command Mode

administrator exec

Syntax Description

list-num	Optional. Number of the AS path access control list.

Default

Displays all configured AS path access lists.

Usage Guidelines

Use the **show as-path-access-list** command without any options to display information on all configured AS path access lists. Use the *list-num* argument to view information about a specific AS path access control list.

Examples

The following example displays two AS path access lists (9 and 22):

```
[local]Redback#show as-path-access-list

AS path access list 9
   sequence 10: permit !3
   sequence 20: permit !15 3+
AS path access list 22
   sequence 10: permit 3{1,3}
   sequence 20: deny 3{1,4}
   sequence 30: permit 3{1,2}
```

Related Commands

as-path access-list

show community-list

show community-list [*list-num*]

Purpose

Displays configured Border Gateway Protocol (BGP) community lists.

Command Mode

administrator exec

Syntax Description

list-num	Optional. Number of a the community list.

Default

Displays all configured community lists.

Usage Guidelines

Use the **show community-list** command without any options to display all configured community lists. Use the *list-number* argument to display information about a specific community list.

Examples

The following example displays two community lists (1 and 2):

```
[local]Redback#show community-list

community-list 1
  sequence 10:permit 3 15
  sequence 20: deny 11 12 21 no-export no-advertise
community-list 2
  sequence 5: permit 65012 4260626443
```

Related Commands

match community-list
set community

show route-access-list

show route-access-list [*list-num*]

Purpose

Displays configured route access control lists.

Command Mode

administrator exec

Default

Displays all configured route access lists.

Syntax Description

list-num	Optional. Number of a specific route access control list.

Usage Guidelines

Use the **show route-access-list** command without the argument to display all configured community lists. Use the *list-number* argument to display information about a specific route access control list.

Examples

The following example displays two route access lists (`10` and `100`):

```
[local]Redback#show route-access-list

route-access-list 10
  sequence 10: deny 200.0.0.0 wildcard bits 0.255.255.255
  sequence 20: permit any
route-access-list 100
  sequence 15: permit 29.0.0.0 0.255.255.255 255.255.0.0 0.255.255.255
```

Related Commands

route-access-list extended-access-list-num
route-access-list standard-access-list-num

show route-map

show route-map [*map-name*]

Purpose

Displays configured route maps.

Command Mode

administrator exec

Syntax Description

map-name	Optional. Name of the route map.

Default

Displays all configured route maps.

Usage Guidelines

Use the **show route-map** command without the argument to list all route maps. Use the *map-name* argument to display a specific route map.

Examples

The following example displays two route maps (`filter-a-bunch` and `set-pref`):

```
[local]Redback#show route-map

route-map filter-a-bunch, permit, sequence 5
  Match clauses:
   as-path (as-path filter): 20 10 1
  Set clauses:
   community 720897
   metric +11

route-map filter-a-bunch, deny sequence 15
  Match clauses:
   community (community-list filter): 3 8 54
   interface enet60
```

```
route-map set-pref, permit, sequence 10
  Match clauses:
   ip address (route-access-lists): 1 101
  Set clauses:
   preference 155
```

Related Commands

match as-path
match community-list
match interface
match ip address
match ip next-hop
match metric
match route-type
match tag
route-map
set as-path prepend
set community
set ip next-hop
set local-preference
set metric
set origin
set preference

Chapter 36

IGMP Proxy Commands

This chapter describes the commands used to configure and maintain Internet Group Management Protocol (IGMP) proxy features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure IGMP, and configuration examples, see the "Configuring IGMP Proxy" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug ip igmp

debug ip igmp

no debug ip igmp

Purpose

Enables the logging of Internet Group Management Protocol (IGMP) debug messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Usage Guidelines

Use the **debug ip igmp** command to enable the logging of IGMP debug messages. You can use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables the logging of IGMP debug messages:

```
[local]RedBack#debug ip igmp
```

Related Commands

counters—ATM configuration mode
counters—Frame Relay configuration modes
ip igmp

ip igmp join-group
ip igmp leave-group
ip multicast receive
ip multicast-routing
ip multicast send
last-member-query-interval
logging console
query-interval
query-response-interval
router-igmp-interface
router igmp-proxy
show ip igmp
show ip igmp
show ip igmp
startup-query-interval
terminal monitor
unsolicited-report-interval
version1-router-interval

def-version

def-version {**1** | **2**}

default def-version

Purpose

Modifies the version of Internet Group Management Protocol (IGMP) that is used on the interface.

Command Mode

IGMP configuration

Syntax Description

1 Sets IGMP to version 1.

2 Sets IGMP to version 2. This is the default value.

Default

The interface uses IGMP version 2.

Usage Guidelines

Use the **def-version** command to modify the IGMP version that is used on the interface.

Use the **default** form of this command to return the IGMP version to IGMPv2.

Examples

The following example sets the IGMP version to `1`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#def-version 1
```

Related Commands

debug ip igmp
last-member-query-interval
query-interval

query-response-interval
robustness
show ip igmp
startup-query-interval
unsolicited-report-interval
version1-router-interval

ip igmp

ip igmp

no ip igmp

Purpose

Enables Internet Group Management Protocol (IGMP) on the interface.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

IGMP is disabled.

Usage Guidelines

Use the **ip igmp** command to enable IGMP on the interface. When IGMP is enabled, the Subscriber Management System (SMS) device originates IGMP queries on the designated interface, and uses IGMP reports from hosts on circuits bound to the interface to build multicast forwarding tables.

You must enable multicast routing using the **ip multicast-routing** command in context configuration mode. And you must enable subscribers through the **ip multicast send** and **ip multicast receive** commands in subscriber configuration mode.

The management port cannot be enabled with IGMP. This command does not apply to loopback interfaces.

Use the **no** form of this command to disable IGMP on the interface.

Examples

The following example enables IGMP on interface `int1`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface int1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
```

Related Commands

debug ip igmp
ip multicast receive
ip multicast-routing
ip multicast send
router-igmp-interface
router igmp-proxy
show ip igmp

ip igmp join-group

ip igmp join-group circuit {*slot/port* {*vpi vci* | *hdlc-channel dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*} *multicast-IP-address*

no ip igmp join-group circuit {*slot/port* {*vpi vci* | *hdlc-channel dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*} *multicast-IP-address*

Purpose

Joins the specified circuit with an Internet Group Management Protocol (IGMP) multicast group.

Command Mode

administrator exec mode
context configuration

Syntax Description

circuit *slot/port*	Slot and port. Used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay I/O modules. The range of values for the *slot* argument is 0 to 31. The range of values for the *port* argument is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI). Used with ATM ports. The range of values for the *vpi* argument is 0 to 255. The range of values for the *vci* argument depends on the I/O module: • ATM T1—1 to 1,023 • ATM DS-3 (version 1)—1 to 2,047 • ATM OC-3 (version 1)—1 to 4,095 • ATM (version 2)—1 to 65,535
hdlc-channel	Name of the High-Level Data Link Control (HDLC) channel on the channelized DS-3 port. This argument is required for channelized DS-3 modules and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) used with Frame Relay ports. The range of values is 16 to 991.
lac *vcn*	Layer 2 Tunneling Protocol Access Controllers (LAC) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.
lns *vcn*	Layer 2 Tunneling Protocol Network Services (LNS) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.

pppoe *cm-slot-session-id*	Point-to-Point Protocol over Ethernet (PPPoE) session. The *cm-slot* argument is required for Connection Manager (CM) modules on the SMS 10000 device and is not used in any other case. It specifies the CM slot number. The *session-id* argument must be specified for all product platforms; the range of values is 1 to 65,534.
multicast-IP-address	IP address of the multicast group that the circuit joins.

Default

None

Usage Guidelines

Use the **ip igmp join-group circuit** command to join the circuit with an IGMP multicast group. The Access Operating System (AOS) maintains a per-context membership table that maps multicast groups to circuits.

Use this command in context configuration mode if you want a circuit to retain membership even after a system reset; use this command in administrator exec mode if you do not want an entry to carry across a system reset.

Link-local multicast IP addresses 224.0.0.0 to 224.0.0.255 cannot be joined.

For IGMP proxy to function, you must enable IP multicasting using the **ip multicast-routing** command in context configuration mode. You must enable at least one interface in the context using the **ip igmp** command in interface configuration mode. You must also enable subscribers through the **ip multicast send** and **ip multicast receive** commands in subscriber configuration mode.

Use the **no** form of this command to drop the circuit; in this manner, you can first verify that the specified circuits are not current members of the multicast group before dropping the circuits. You can use the **ip igmp leave-group** command in administrator exec mode to drop circuits; circuits are dropped immediately, even if they are current members of the multicast group.

Examples

The following example joins the circuit at slot and port numbers `3/0` using a VPI of `24` and a VCI of `16` with the multicast group at IP address `234.128.64.32`:

```
[local]RedBack(config-ctx)#ip igmp join-group circuit 3/0 234.128.64.32
```

The following example drops the circuit at slot and port numbers `3/0` using a VPI of `24` and a VCI of `16` with the multicast group at IP address `234.128.64.32:`

```
[local]RedBack#no ip igmp join-group circuit 3/0 234.128.64.32
```

Related Commands

debug ip igmp
ip igmp leave-group
ip multicast max-groups

ip multicast receive
ip multicast-routing
ip multicast send
show ip igmp

ip igmp leave-group

ip igmp leave-group circuit {*slot/port* {*vpi vci* | *hdlc-channel dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*} *multicast-IP-address* | **all**

no ip igmp leave-group circuit {*slot/port* {*vpi vci* | *hdlc-channel dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*} *multicast-IP-address* | **all**

Purpose

Drops one or more circuits from an Internet Group Management Protocol (IGMP) multicast group.

Command Mode

administrator exec

Syntax Description

circuit *slot/port*	Slot and port. Used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay I/O modules. The range of values for the *slot* argument is 0 to 31. The range of values for the *port* argument is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI). Used with ATM ports. The range of values for the *vpi* argument is 0 to 255. The range of values for the *vci* argument depends on the I/O module: • ATM T1—1 to 1,023 • ATM DS-3 (version 1)—1 to 2,047 • ATM OC-3 (version 1)—1 to 4,095 • ATM (version 2)—1 to 65,535
hdlc-channel	Name of the High-Level Data Link Control (HDLC) channel on the channelized DS-3 port. This argument is required for channelized DS-3 modules and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) used with Frame Relay ports. The range of values is 16 to 991.
lac *vcn*	Layer 2 Tunneling Protocol Access Controllers (LAC) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.
lns *vcn*	Layer 2 Tunneling Protocol Network Services (LNS) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.

pppoe *cm-slot-session-id*	Point-to-Point Protocol over Ethernet (PPPoE) session. The *cm-slot* argument is required for Connection Manager (CM) modules on the SMS 10000 device and is not used in any other case. It specifies the CM slot number. The *session-id* argument must be specified for all product platforms; the range of values is 1 to 65,534.
multicast-IP-address	IP address of the multicast group from which the circuit is dropped.
all	Causes all entries in the multicast membership table to be cleared.

Default

None

Usage Guidelines

Use the **ip igmp leave-group** command to drop one or more circuits from multicast group. The Access Operating System (AOS) maintains a membership table mapping multicast groups to circuits. This command clears specific entries or all entries in this table for the current context.

Caution Circuits are dropped immediately. In context configuration mode, you can use the **no ip igmp join-group circuit** command to ensure that there are no current members in the multicast group before dropping the circuits.

When a circuit is specified, it is removed from the membership list for the multicast group. Otherwise, all circuits associated are removed from the membership list. When a circuit is specified along with the **all** keyword, the specified circuit is removed from the membership list for all groups in the table. When the keyword **all** is used alone, all entries from the membership table are removed.

Link-local addresses (224.0.0.1 to 224.0.0.255) cannot be deleted from the table.

For Internet Group Management Protocol (IGMP) proxy to function, you must enable IP multicasting using the **ip multicast-routing** command in context configuration mode. You must enable at least one interface in the context with IGMP using the **ip igmp** command in interface configuration mode. You must also enable subscribers through the **ip multicast send** and **ip multicast receive** commands in subscriber configuration mode.

Examples

The following example clears all entries in the multicast membership table:

```
[local]RedBack#ip igmp leave-group all
```

Related Commands

debug ip igmp
ip igmp
ip igmp join-group
ip multicast receive

ip multicast-routing
ip multicast send
show ip igmp

ip igmp mode

ip igmp mode

Purpose

Enters Internet Group Management Protocol (IGMP) configuration mode.

Command Mode

interface configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **ip igmp mode** command to enter IGMP configuration mode.

Examples

The following example causes the system to enter IGMP configuration mode:

```
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#
```

Related Commands

ip igmp

ip multicast max-groups

ip multicast max-groups *max-count*

no ip multicast max-groups

Purpose

Limits the number of IP multicast groups that a subscriber can join.

Command Mode

subscriber configuration

Syntax Description

max-count	Number of multicast groups a subscriber can join. The range of values is 1 to 4,294,967,295.

Default

There is no limit on the number of groups a subscriber can join.

Usage Guidelines

Use the **ip multicast max-groups** command to limit the number of IP multicast groups that a subscriber can join.

To configure a maximum number of groups that a context can contain, use the **ip multicast-routing** command.

Use the **no** form of this command to reset the number of groups that a subscriber can join to unlimited.

Examples

The following example restricts the subscriber named `susan` to be a member of a maximum of three multicast groups:

```
[local]RedBack(config-ctx)#subscriber name susan
[local]RedBack(config-sub)#ip multicast max-groups 3
```

Related Commands

ip multicast receive
ip multicast-routing
ip multicast send
show ip igmp

ip multicast receive

ip multicast receive {**permit** | **deny**}

no ip multicast receive

Purpose

Configures the multicast receive permissions for a single subscriber record or for a default subscriber record.

Command Mode

subscriber configuration

Syntax Description

permit	Allows the subscriber to receive multicast traffic.
deny	Denies the subscriber the ability to receive multicast traffic.

Default

The multicast receive permission is set to **deny**.

Usage Guidelines

Use the **ip multicast receive** command to configure the multicast receive permissions for a single subscriber record or for a default subscriber record. Permission attributes are applied in the following order: subscriber record, default subscriber record, and system defaults. If a permission is not defined in the subscriber record, it inherits the value of the permission from the default subscriber record. If the permission is not defined in the default subscriber record, the system default values are used.

For Internet Group Management Protocol (IGMP) proxy to function, you must enable IP multicasting using the **ip multicast-routing** command in context configuration mode. You must enable at least one interface in the context with IGMP using the **ip igmp** command in interface configuration mode. You must also enable subscribers through the **ip multicast send** and **ip multicast receive** commands in subscriber configuration mode.

Use the **no** form of this command to delete receive permissions for the profile to which the command is applied.

Examples

The following example sets receive permissions to `permit` for the default subscriber record:

```
[local]RedBack(config-ctx)#subscriber default
[local]RedBack(config-sub)#ip multicast receive permit
```

The following example sets receive permissions to `deny` for subscriber `freddy`:

```
[local]RedBack(config-ctx)#subscriber name freddy
[local]RedBack(config-sub)#ip multicast receive deny
```

Related Commands

ip igmp
ip multicast max-groups
ip multicast-routing
ip multicast send
show ip igmp

ip multicast-routing

ip multicast-routing [*max-groups*]

no ip multicast-routing

Purpose

Enables IP multicast routing for the context and, optionally, sets a limit on the number of multicast groups allowed.

Command Mode

context configuration

Syntax Description

max-groups	Optional. Maximum number of multicast groups allowed in the context. The range of values is 1 to 65,536. The default is 65,536.

Default

IGMP proxy is disabled.

Usage Guidelines

Use the **ip multicast-routing** command to enable IP multicast routing for the context. Use the *max-groups* argument to configure a maximum number of multicast groups allowed in the context.

To configure a maximum number of groups that a subscriber can join, use the **ip multicast max-groups** command in subscriber configuration mode.

For Internet Group Management Protocol (IGMP) proxy to function, you must enable IP multicasting using the **ip multicast-routing** command in context configuration mode. You must enable at least one interface in the context with IGMP using the **ip igmp** command in interface configuration mode. You must also enable subscribers through the **ip multicast send** and **ip multicast receive** commands in subscriber configuration mode.

Use the **no** form of this command to disable IP multicast routing. When multicast routing is disabled, the system stops generating IGMP queries and does not maintain multicast forwarding information. Multicast data originating from subscribers is dropped.

Examples

The following example enables IP multicast routing for the context `bigisp`:

```
[local]RedBack(config)#context bigisp
[local]RedBack(config-ctx)#ip multicast-routing
```

Related Commands

debug ip igmp
ip igmp
ip multicast receive
ip multicast-routing
ip multicast send
show ip igmp

ip multicast send

ip multicast send {**permit** [**unsolicit**] | **deny**}

no ip multicast send

Purpose

Configures the multicast send permissions for a subscriber record or for the default subscriber record.

Command Mode

subscriber configuration

Syntax Description

permit	Allows the subscriber to send multicast traffic.
unsolicit	Optional. Used in conjunction with the **permit** keyword to indicate that the subscriber is allowed to send unsolicited multicast traffic.
deny	Denies the subscriber the ability to send multicast traffic.

Default

The multicast send permission is set to deny.

Usage Guidelines

Use the **ip multicast send** command to configure the multicast send permissions for a subscriber record or for the default subscriber record.

If the **permit** keyword is used without the **unsolicit** keyword, the subscriber must join a group prior to sending unsolicited multicast data. If used together (**permit unsolicit**), a subscriber is allowed to send unsolicited multicast traffic. Permissions are examined in the following order: subscriber record, default subscriber record, and system defaults. If a permission is not defined in the subscriber record, it inherits the value of the permission from the default subscriber record. If the permission is undefined in the default subscriber record, the system default values are used.

For Internet Group Management Protocol (IGMP) proxy to function, you must enable IP multicasting using the **ip multicast-routing** command in context configuration mode. You must enable at least one interface in the context with IGMP using the **ip igmp** command in interface configuration mode. You must also enable subscribers through the **ip multicast send** and **ip multicast receive** commands in subscriber configuration mode.

Use the **no** form of this command to delete all send permissions for the profile. Deleting the permissions in a subscriber record causes the system to use the permissions from the default subscriber record. If no such permissions exist in the default subscriber record, the system default is used.

Examples

The following example configures the default subscriber record with the permission to send multicast traffic; however, subscriber `mike` is denied sending multicast traffic:

```
[local]RedBack(config-ctx)#subscriber default
[local]RedBack(config-sub)#ip multicast send permit
[local]RedBack(config-sub)#exit
[local]RedBack(config-ctx)#subscriber name mike
[local]RedBack(config-sub)#ip multicast send deny
```

The following example using the **no** form deletes send permissions in the default subscriber record. In this case, the system default settings are used. Therefore, subscriber `jane` cannot send or receive multicast traffic.

```
[local]RedBack(config-ctx)#subscriber default
[local]RedBack(config-sub)#no ip multicast send
[local]RedBack(config-sub)#exit
[local]RedBack(config-ctx)#subscriber name jane
[local]RedBack(config-sub)#ip address 10.10.1.4
[local]RedBack(config-sub)#exit
```

Related Commands

debug ip igmp
ip multicast max-groups
ip multicast receive
ip multicast-routing
ip multicast send
show ip igmp

last-member-query-interval

last-member-query-interval {**count** *packets* [**timer** *interval*] | **timer** *interval*}

default last-member-query-interval

Purpose

Modifies the interval and count for Internet Group Management Protocol (IGMP) version 2 queries sent by multicast group members.

Command Mode

IGMP configuration

Syntax Description

count *packets*	Number of packets sent out as part of the last member query. The range of values is 1 to 10. The default value is 2.
timer *interval*	Last member query interval in tenths of a second. (100 indicates that the interval is 10 seconds.) The range of values is 1 to 864,000. The default value is 10 (1 second).

Default

The timer value is 10 (1 second) and the count value is 2 packets.

Usage Guidelines

Use the **last-member-query-interval** command to modify the interval and count for IGMP version 2 queries sent by multicast group members. The timer can be tuned to modify the leave latency of the network. A smaller value results in quicker detection of the loss of the last member of a group. The count value is the number of times group-specific queries are sent before the Access Operating System (AOS) determines that there are no more members using the circuit.

Typically, these values are left at their default setting.

Use the **default** form of this command to return the values to their default settings.

Examples

The following example sets the interval to `20` (or 2 seconds) and sets the packet count to `3`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#last-member-query-interval timer 20 count 3
```

Related Commands

def-version
query-interval
query-response-interval
robustness
show ip igmp
startup-query-interval
unsolicited-report-interval
version1-router-interval

query-interval

query-interval timer *interval*

default query-interval timer

Purpose

Modifies the interval between Internet Group Management Protocol (IGMP) queries sent on the subnet.

Command Mode

IGMP configuration

Syntax Description

timer *interval*	Interval, in seconds, between IGMP queries sent. The range of values is 1 to 86,400. The default value is 125.

Default

The interval is 125 seconds.

Usage Guidelines

Use the **query-interval** command to modify the interval between IGMP queries sent on the subnet. By varying the interval, you can tune the number of IGMP messages on the subnet. Larger values cause IGMP queries to be sent less often. There is typically no requirement to change this value.

Use the **default** form of this command to return the interval to 125 seconds.

The **query-interval** command's value is also returned to its default setting if the **query-response-interval** command's value is greater than the value of the **query-interval** command's value. If the default interval of 125 seconds is less than the **query-response-interval** command's value, the **query-response-interval** value is reset to its default value (10 seconds).

Examples

The following example sets the IGMP query interval to `180` seconds:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#query-interval timer 180
```

Related Commands

def-version
last-member-query-interval
query-response-interval
robustness
show ip igmp
startup-query-interval
unsolicited-report-interval
version1-router-interval

query-response-interval

query-response-interval timer *interval*

default query-response-interval timer

Purpose

Modifies the maximum time allowed for a host on a subnet to send a response to an Internet Group Management Protocol (IGMP) query.

Command Mode

IGMP configuration

Syntax Description

timer *interval*	Amount of time, in tenths of a second, after which a host must send a response. A value of 100 indicates that the interval is 10 seconds. The range of values is 1 to 864,000. The default value is 100 (10 seconds).

Default

The interval is 100 tenths of a second (10 seconds).

Usage Guidelines

Use the **query-response-interval** command to modify the maximum time allowed for a host on a subnet to send a response to an IGMP query. By varying the interval, you can tune the burstiness of IGMP messages on the subnet. A larger value makes the traffic less bursty, because host responses are spread out over a longer interval. This value for this command must be less than the value that is configured using the **query-interval** command.

Use the **default** form of this command to return the value to its default setting. The value is typically left at its default setting.

If you return the **query-response-interval** to its default value and the value set via the **query-interval** command is less than the default **query-response-interval** (10 seconds), the value for the **query-interval** command is returned to its default value of 125 seconds. This transition occurs transparently without notification.

Examples

The following example shows the IGMP query response interval set to `300` (30 seconds):

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#query-response-interval timer 300
```

Related Commands

debug ip igmp
def-version
last-member-query-interval
query-interval
robustness
show ip igmp
startup-query-interval
unsolicited-report-interval
version1-router-interval

robustness

robustness *value*

default robustness

Purpose

Configures the expected packet loss for the specified Internet Group Management Protocol (IGMP) interface.

Command Mode

IGMP configuration

Syntax Description

value	Degree of robustness. The range of values 1 to 10. The value of 1 is not recommended. The default value is 2.

Default

The robustness value is 2.

Usage Guidelines

Use the **robustness** command to configure the expected packet loss for the specified IGMP interface. If a subnet is expected to be lossy, the robustness value can be increased.

Use the **default** form of this command to return the robustness value to its default setting.

Examples

The following example sets the IGMP robustness value to 4:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#robustness 4
```

Related Commands

debug ip igmp
def-version
last-member-query-interval
query-interval
query-response-interval
show ip igmp
startup-query-interval
unsolicited-report-interval
version1-router-interval

router-igmp-interface

router-igmp-interface *if-name*

no router-igmp-interface *if-name*

Purpose

Configures Internet Group Management Protocol (IGMP) proxy on the interface that is attached to a multicast router.

Command Mode

IGMP proxy router configuration

Syntax Description

if-name	Name of the interface that is to be connected to the multicast router.

Default

None

Usage Guidelines

Use the **router-igmp-interface** command to configure IGMP proxy on the interface that is attached to a multicast router. All multicast data and IGMP reports are sent out on the circuit associated with the multicast router interface.

Only one interface per context can be configured as the interface that connects to the multicast router. If this command is repeated on a second interface, the second interface becomes the multicast router interface and information about the first interface is deleted. The multicast router interface can only be bound to a single circuit.

The interface that is connected to the multicast router cannot be enabled with IGMP via the **ip igmp** command. This command does not apply to loopback interfaces.

Use the **no** form of this command to delete the multicast router designation on the interface.

Examples

The following example configures the interface `bb1` as the interface to which the multicast router is attached:

```
[local]RedBack(config-ctx)#router igmp-proxy
[local]RedBack(config-router-igmp)#router-igmp-interface bb1
```

Related Commands

debug ip igmp
ip igmp
router igmp-proxy
show ip igmp

router igmp-proxy

router igmp-proxy

Purpose

Enters Internet Group Management Protocol (IGMP) proxy router configuration mode.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **router igmp-proxy** command to enter IGMP proxy router configuration mode, where the interface to which the multicast-capable router is attached can be configured via the **router-igmp-interface** command in IGMP proxy router configuration mode.

Examples

The following example enters IGMP proxy router configuration mode:

```
[local]RedBack(config-ctx)#router igmp-proxy
[local]RedBack(config-router-igmp)#
```

Related Commands

router-igmp-interface

show ip igmp

show ip igmp [**circuit** {*slot/port* {*vpi vci* | *hdlc-channel dlci*}| **lac** *vcn* | **lns** *vcn* | **pppoe** *cm-slot-session-id*} *multicast-IP-address* | **group** [*multicast-IP-address* [**verbose**]] | **interface** *if-name* [**verbose**] | **params** [**interface** *if-name*] | **subscriber** [**name** *sub-name*]]

Purpose

Displays Internet Group Management Protocol (IGMP) proxy information.

Command Mode

operator exec

Syntax Description

circuit *slot/port*	Slot and port. Used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay I/O modules. The range of values for the *slot* argument is 0 to 31. The range of values for the *port* argument is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI). Used with ATM ports. The range of values for the *vpi* argument is 0 to 255. The range of values for the *vci* argument depends on the I/O module: • ATM T1—1 to 1,023 • ATM DS-3 (version 1)—1 to 2,047 • ATM OC-3 (version 1)—1 to 4,095 • ATM (version 2)—1 to 65,535
hdlc-channel	Name of the High-Level Data Link Control (HDLC) channel on the channelized DS-3 port. This argument is required for channelized DS-3 modules and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) used with Frame Relay ports. The range of values is 16 to 991.
lac *vcn*	Layer 2 Tunneling Protocol Access Controllers (LAC) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.
lns *vcn*	Layer 2 Tunneling Protocol Network Services (LNS) virtual circuit number (VCN). The range of values for the SMS 1800 device and SMS 500 device is 0 to 65,534. The range of values for the SMS 10000 device is 0 to 131,068.

pppoe *cm-slot-session-id*	Point-to-Point Protocol over Ethernet (PPPoE) session. The *cm-slot* argument is required for Connection Manager (CM) modules on the SMS 10000 device and is not used in any other case. It specifies the CM slot number. The *session-id* argument must be specified for all product platforms; the range of values is 1 to 65,534.
multicast-IP-address	IP address of the multicast group from which the circuit is dropped.
group	Optional. Displays group information, such as number of members.
verbose	Optional. Lists individual member circuits.
interface *if-name*	Interface for which information is to be displayed.
params	Optional. Displays the IGMP parameters configured for each interface or for a specified interface.
subscriber	Optional. Displays information on all subscribers unless a name is specified.
name *sub-name*	Name of the subscriber for which information is displayed.

Default

None

Usage Guidelines

You can use the various forms of the **show ip igmp** command to list general information on IGMP proxy, subscribers, interfaces, and circuits, or to display details specific to any of these areas.

Examples

The following example displays IGMP parameters for all interfaces:

```
[local]RedBack>show ip igmp params

IGMP Parameters for interface atm40
IGMP version:2                    Robustness value:           2
Query interval:125(s)             Query response interval:  100(t)
Startup query interval:31(s)      Startup query count:        2
Last member query interval:10(t)  Last member query count:    2
Unsolicited report interval:10(s) Version1-router-present:  400(s)

IGMP Parameters for interface enet60
IGMP version: 2                   Robustness value:           2
Query interval:125(s)             Query response interval:  100(t)
Startup query interval:31(s)      Startup query count:        2
Last member query interval:10(t)  Last member query count:    2
Unsolicited report interval:10(s) Version1-router-present:  400(s)
```

The following example displays IGMP parameters for a single interface:

```
[local]RedBack>show ip igmp params interface enet60

IGMP Parameters for interface enet60
IGMP version:2                    Robustness value:           2
Query interval:125(s)             Query response interval:   100(t)
Startup query interval:31(s)      Startup query count:         2
Last member query interval:10(t)  Last member query count:     2
Unsolicited report interval:10(s) Version1-router-present:   400(s)
```

In the following example, the number of members associated with all active multicast group addresses is displayed. The `Router Attached` column indicates whether or not a router is attached and a multicast circuit is enabled for forwarding packets.

```
[local]RedBack>show ip igmp group

Current group count: 2
  Groups             Count    Router Attached
-----------------    -------  ----------------
  225.1.1.2          7        NO
  228.1.1.1          1        NO
```

The following example lists detailed statistics for each multicast group. The `current group count` field indicates the number of members in a group. The `router cct?` field provides information on whether or not an interface is attached to a network on which a multicast router is present.

```
[local]RedBack>show ip igmp group verbose

current group count: 3
=============================================================================
 Group: 225.1.1.2                           Members:3
  Interface: atm40                          Member count:3
  Local members: 0                          Last Reporter:0.0.0.0
  Up time 49686 days,12 hrs,56 mins,9 secs Expiration time 0 secs
   circuit: 4/0 1 3
    access permission: snd: ON  unsol-snd: ON  rcv: ON
    max groups: UNLIMITED current groups: 1  router cct? NO
    multicast cct entry: flags: [ forward valid ]
    multicast cct delete time 0 (secs)
   circuit: 4/0 1 4
    access permission: snd: ON unsol-snd: ON rcv: ON
    max groups: UNLIMITED current groups: 1  router cct? NO
    multicast cct entry: flags: [ forward valid ]
    multicast cct delete time 0 (secs)
   circuit: 4/0 1 7
    access permission: snd: ON unsol-snd: ON rcv: ON
    max groups: UNLIMITED current groups: 1  router cct? NO
    multicast cct entry: flags: [ forward valid ]
    multicast cct delete time 0 (secs)
=============================================================================
```

```
 Group: 227.5.5.1                              Members: 1
  Interface: enet60                            Member count: 1
  Local members: 0                             Last Reporter: 155.53.147.1
  Up time 49686 days,12 hrs,56 mins,2 secs Expiration time 163 secs
   circuit: 6/0
    access permission: snd: ON unsol-snd: ON rcv: ON
    max groups:UNLIMITED current groups: 2 router cct? NO
    multicast cct entry: flags: [ forward valid ]
    multicast cct delete time 150 (secs)
=====================================================================
 Group: 225.5.5.2                              Members: 1
  Interface: enet60                            Member count:1
  Local members: 0                             Last Reporter:155.53.147.1
  Up time 49686 days,12 hrs,56 mins,9 secs Expiration time 160 secs
   circuit: 6/0
    access permission: snd: ON   unsol-snd: ON rcv: ON
    max groups: UNLIMITED  current groups: 8     router cct? NO
    multicast cct entry: flags: [ forward valid ]
    multicast cct delete time 0 (secs)
```

The following example displays statistics for the multicast group at IP address `255.1.1.2`. The `Count` column indicates the number of members in the group.

```
[local]RedBack>show ip igmp group 225.1.1.2

  Groups             Count    Router Attached
  -----------------  -------  ----------------
  225.1.1.2          7        YES
```

The following example displays statistics for all circuits belonging to an interface:

```
[local]RedBack>show ip igmp interface atm40

  Circuits                SND/UNS-SND/RCV    Groups
 ----------------------   ----------------   ----------------
  4/0 1 4                 ON  OFF     ON     225.1.1.2

  4/0 1 3                 ON  ON      ON     225.1.1.2

  4/0 1 7                 OFF OFF     ON     225.1.1.2

  4/0 1 6                 OFF OFF     ON
  4/0 1 5                 OFF OFF     ON
  4/0 1 2                 OFF OFF     ON
  4/0 1 1                 OFF OFF     ON
```

The following example displays additional details specific to the `atm40` interface using the **verbose** keyword:

```
[[local]RedBack>show ip igmp interface atm40 verbose

circuit: 4/0 1 4
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 1   router cct? NO
     group: 225.1.1.2
circuit: 4/0 1 3
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 1   router cct? NO
     group: 225.1.1.2
circuit: 4/0 1 7
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 1   router cct? NO
      group: 225.1.1.2
circuit: 4/0 1 6
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 0   Circuit Disabled
circuit: 4/0 1 5
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 0   Circuit Disabled
circuit: 4/0 1 2
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 0   Circuit Disabled
circuit: 4/0 1 1
     access permission: snd: ON unsol-snd: ON   rcv: ON
     max groups: UNLIMITED current groups: 0   Circuit Disabled
```

The following example displays statistics for a specific circuit used for IGMP proxy. The `Local` field indicates whether or not the group was joined locally (for example, with the **ip igmp join-group circuit** command). The `Forward` field indicates whether or not packets are forwarded to group members.

```
[local]RedBack>show ip igmp circuit 4/0 1 7

circuit: 4/0 1 7
 access permission: snd:OFF unsol-snd:OFF rcv:ON
 max groups: UNLIMITED       current group: 1   router cct? NO

    Groups            Local  Forward
    ----------------- -----  -------
    225.1.1.2         OFF    ON
```

The following example displays a list of all subscribers using IGMP proxy:

```
[local]RedBack>show ip igmp subscriber

  Groups             Circuits                 Subscribers
  -------------------------------------------------------
  225.1.1.2          4/1 1 1                  b01@sender
  225.1.1.2          4/1 1 2                  b02@sender
  225.1.1.2          4/1 1 3                  b03@sender
  225.1.1.2          4/1 1 4                  b04@sender
  225.1.1.2          4/1 1 5                  b05@sender
  225.1.1.2          4/1 1 6                  b06@sender
```

The following example displays statistics for a specific subscriber:

```
[local]RedBack>show ip igmp subscriber name b06@local

Subscriber name b06@local:
circuit: 4/1 1 6
  access permission: snd:ON  unsol-snd:ON        rcv:OFF
  max groups: UNLIMITED current groups:2         router cct? YES

Groups             Local  Forward
------------------ -----  -------
226.1.1.3          OFF    ON
225.1.1.2          OFF    ON
```

Related Commands

debug ip igmp
ip igmp
ip igmp join-group
ip igmp leave-group
ip multicast max-groups
ip multicast receive
ip multicast-routing
ip multicast send
last-member-query-interval
query-interval
query-response-interval
robustness
router-igmp-interface
router igmp-proxy
startup-query-interval
unsolicited-report-interval
version1-router-interval

startup-query-interval

startup-query-interval count {**count** *packets* [**timer** *interval*] | **timer** *interval*}

default startup-query-interval

Purpose

Sets the interval between Internet Group Management Protocol (IGMP) queries sent through the interface when a circuit is brought up.

Command Mode

IGMP configuration

Syntax Description

count *packets*	Specifies the number of packets sent out as part of the startup query. The range is 1 through 10.
timer *interval*	Specifies the startup query interval in tenths of a second. For example, a *timeval* of 100 indicates that the interval is 10 seconds. The range is 1 through 864,000. The default value is **query-interval**/4.

Default

The **timer** *value* is query-interval/4. For example, if the **query-interval** command is set to its default value of 125 seconds, the startup query interval is 31 seconds. The **count** *value* is equal to the **robustness** value.

Usage Guidelines

Use the **startup-query-interval** command to set the interval between IGMP queries sent through the interface when a circuit is brought up. A total of **count** *packet* packets are sent spaced apart by the **timer** *interval*. This interval enables the Subscriber Management System (SMS) device to quickly detect the presence of the various multicast groups on each of the circuits.

Use the **default** form of this command to return the values to their default settings. These values are typically left at the default settings.

Examples

The following example sets the startup query interval to `250` (25 seconds) with a packet count of `3`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#startup-query-interval timer 250 count 3
```

Related Commands

debug ip igmp
def-version
last-member-query-interval
query-interval
query-response-interval
robustness
show ip igmp
unsolicited-report-interval
version1-router-interval

unsolicited-report-interval

unsolicited-report-interval timer *interval*

default unsolicited-report-interval timer

Purpose

Sets the interval between unsolicited Internet Group Management Protocol version 2 (IGMPv2) reports sent by the Subscriber Management System (SMS) device to the IP multicast router.

Command Mode

IGMP configuration

Syntax Description

timer *interval*	Unsolicited report interval in seconds. The range of values is 1 through 86,400. The default is 10.

Default

The interval between unsolicited IGMPv2 reports sent by the SMS device to the IP multicast router is 10 seconds.

Usage Guidelines

Use the **unsolicited-report-interval timer** command to set the interval between unsolicited IGMPv2 reports sent by the SMS to the router.

Use the **default** form of this command to return the interval to its default setting. This value is typically left at its default setting.

Examples

The following example sets the IGMP unsolicited-report interval to `15` seconds:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#unsolicited-report-interval timer 15
```

Related Commands

debug ip igmp
def-version
last-member-query-interval
query-interval
query-response-interval
robustness
show ip igmp
startup-query-interval
version1-router-interval

version1-router-interval

version1-router-interval timer *interval*

default version1-router-interval timer

Purpose

Configures the period of time that the interface must wait after hearing an Internet Group Management Protocol version 1 (IGMPv1) query before sending out an IGMP version 2 (IGMPv2) message.

Command Mode

IGMP configuration

Syntax Description

timer *interval*	Specifies the waiting period in seconds. The range is 1 through 86,400. The default value is 400 seconds.

Default

By default, the value is 400 seconds.

Usage Guidelines

Use the **version1-router-interval timer** command to configure the period of time that the interface must wait after hearing an IGMPv1 query before sending out an IGMPv2 message. This timer is reset every time an IGMPv1 query is received from the IP multicast router.

Use the **default** form of this command to return the value to its default setting. This value is typically left at its default setting.

Examples

The following example sets the waiting period to `500` seconds:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#interface sub1
[local]RedBack(config-if)#ip address 10.10.32.5 255.255.255.0
[local]RedBack(config-if)#ip igmp
[local]RedBack(config-if)#ip igmp mode
[local]RedBack(config-igmp)#version1-router-interval timer 500
```

Related Commands

debug ip igmp
def-version
last-member-query-interval
query-interval
query-response-interval
robustness
show ip igmp
startup-query-interval
unsolicited-report-interval

Part 10

Access Control Lists

IP Access Control List Commands

This chapter describes the commands related to building and editing IP access control lists using the Access Operating System (AOS). An access control list is a series of statements that define the criteria used to determine whether a packet should be allowed to pass. Use the **ip access-list** context configuration mode command to enter access control list configuration mode. This command requires the name of a new or existing access control list. All subsequent access control list configuration commands are applied to the access list you specify when you enter the mode.

Each access control list configuration command creates a statement in the access control list. When the access control list is applied (to a context, subscriber, or interface), the action performed by each statement is one of the following:

- A **permit** statement causes any packet matching the criteria to be accepted.
- A **deny** statement causes any packet matching the criteria to be dropped.
- A **redirect** statement causes any packet matching the criteria to be forwarded to the specified *next-hop* through the specified *interface*, regardless of the contents of the forwarding table.

All access control lists have an implicit **deny any** command at the end. A packet that does not match the criteria of the first statement is subjected to the criteria of the second statement, and so on, until the end of the access control list is reached; at which point, the packet is dropped.

When used without a prefix, each **deny**, **permit**, or **redirect** command creates a new statement in the access control list. When used with the **before**, **after**, or **no** prefix, each command identifies an existing statement in the access control list.

The **before** and **after** prefixes are positioning prefixes. They indicate where in the access control list you want to insert additional statements. For example, if your access control list already consists of five statements and you want to insert more statements between the third and fourth, you would first use the **after** prefix, specifying the third statement (or the **before** prefix, specifying the fourth statement). The next new statement you create is then inserted between the original third and fourth statements. The next new statement is inserted after that one, and so on, until you provide a different positioning command. Without the instruction provided by a positioning command, each new statement you create is appended after the statement you created before it. Without any positioning commands at all, each new statement is appended to the end of the access control list.

The **no** form of an access control list configuration command identifies and removes an individual statement from the access control list. To delete an entire access control list, you would have to enter context configuration mode, and use the **no** form of the **ip access-list** command, naming the access list to be deleted. To disassociate an access list from the context, interface, or subscriber to which it was applied, you would have to enter the appropriate mode, and use the **no** form of the **ip access-group** command.

For overview information, a description of the tasks used to configure IP access control lists, and configuration examples, see the "Configuring IP Access Control Lists" chapter in the *Access Operating System (AOS) Configuration Guide*.

aaa authorization access-list

aaa authorization access-list radius

default aaa authorization access-list

Purpose

Specifies that an access control list can be downloaded from a Remote Authentication Dial-In User Service (RADIUS) server, if the access control list does not exist in the local configuration.

Command Mode

context configuration

Syntax Description

radius	Specifies that access control lists can be downloaded from the RADIUS server.

Default

Downloading of access control lists from a RADIUS server is disabled for the context.

Usage Guidelines

Use the **aaa authorization access-list** command to enable the downloading of an access control list from the RADIUS server in the event that a requested access control list does not exist in the local configuration. Once an access control list is downloaded from the RADIUS server, it remains available until no more bound subscribers reference it. At that time, the list is deleted from the system.

Use the **clear access-list** command to dereference one or all downloaded access control lists from bound subscribers. The **no ip access-list** command has no effect on downloaded access control lists.

Use the **default** form of this command to disable downloading of access control lists from the RADIUS server.

Note This command description also appears in Chapter 40, “AAA Commands.”

Examples

The following command configures the context `shore` so that the Access Operating System (AOS) looks for an access control list via RADIUS when there is no locally defined access list that matches the name specified:

```
[local]RedBack(config-config)#context shore
[local]RedBack(config-ctx)#aaa authorization access-list radius
```

Related Commands

clear access-list
show ip access-list

access-list undefined

access-list undefined {**permit-all** | **deny-all**}

default access-list undefined

Purpose

Specifies how packets are to be handled (forwarded or dropped) when an undefined access control list is applied to a subscriber or to an interface within a context.

Command Mode

context configuration

Syntax Description

permit-all	Specifies that all packets should be forwarded when an undefined access control list has been applied to a subscriber or interface.
deny-all	Specifies that all packets should be dropped when an undefined access control list has been applied to a subscriber or interface.

Default

All packets are permitted.

Usage Guidelines

Use the **access-list undefined** command to specify how packets are to be handled when an undefined access control list is encountered. It is helpful to have this command in the configuration in cases where an access control list that has not yet been configured is applied to an interface or subscriber, or in cases where an incorrectly named access control list is applied. You can determine whether traffic intended for the interface or subscriber, in such an instance, is forwarded or dropped. Once a defined access control list is applied to the interface or subscriber, traffic can be transmitted according to the parameters of that access control list.

Use the **ip access-list** command in subscriber or interface configuration mode to create an access control list. Use the **ip access-group** command in interface configuration mode to apply the access control list to an interface. Use the **ip access-group** command in subscriber configuration mode to apply the access control list to a subscriber. Use the **ip access-group** command in context configuration mode to apply the access control list to a context (administrative access control list).

Use the **default** form of this command to specify that all packets are to be forwarded when an undefined access control list has been applied to a subscriber or interface.

Examples

The following example sets the **access-list undefined** command to **deny-all** for the local context, and defines an access control list called `NoWebSourcing`. `NoWebSourcing` prohibits a subscriber from hosting web pages at the default HTTP port (TCP port 80):

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#access-list undefined deny-all
[local]RedBack(config-ctx)#ip access-list NoWebSourcing
[local]RedBack(config-ctx)#deny tcp any any eq 80
[local]RedBack(config-ctx)#permit any
```

The following example shows that the administrator, intending to apply the access control list called `NoWebSourcing` to the subscriber named `joe`, types the name as `NoHttpSourcing`:

```
[local]RedBack(config-ctx)#subscriber name joe
[local]RedBack(config-sub)#ip access-group NoHttpSourcing out
```

The result is that packets intended for the subscriber are dropped. If the **access-list undefined** command had been omitted (or set to **permit-all)**, all packets would have been forwarded.

Related Commands

ip access-group
ip access-list

clear access-list

clear access-list *ctx-name* [*list-name*]

Purpose

Dereferences one or all downloadable access control lists from bound subscribers.

Command Mode

operator exec

Syntax Description

ctx-name	Context in which to clear downloadable access lists.
list-name	Optional. Name of the downloadable access list to clear.

Default

No access lists are cleared.

Usage Guidelines

A downloadable access control list is one that has been downloaded from a Remote Authentication Dial-In User Service (RADIUS) server when a requested access control list name does not exist in the local configuration. Downloadable access lists remain loaded as long as subscribers are referencing them. When no more subscribers are referencing a list, it is deleted from the system.

Use the **clear access-list** command to dereference all downloadable access lists in a context, or one specific access list in the context from all bound subscribers. This allows you to update the access control list and have all referencing subscribers use the updated version. The default access control list (as set by the **access-list undefined** command) is applied in the brief interim between authorization and downloading of the access control list from the RADIUS server, and between clearing the access list and downloading the revised one.

If you attempt to use this command to clear a locally configured access list, you see an error message.

Examples

The following example clears all downloadable access lists in the `summer` context from bound subscribers:

```
[local]RedBack#clear access-list summer
```

Related Commands

aaa authorization access-list
access-list undefined
show ip access-list

ip access-group

ip access-group *group-name* {**in** | **out**}

no ip access-group *group-name*

Purpose

Assigns an IP access control list to packets associated with a context, an interface, or a subscriber's circuit.

Command Mode

context configuration
interface configuration
subscriber configuration

Syntax Description

group-name	Name of the IP access control list to apply to the subscriber circuit. Can be a locally configured access list or one that is to be downloaded from a Remote Authentication Dial-In User Service (RADIUS) server.
in	Applies the access group to packets received by the subscriber's circuit.
out	Applies the access group to packets sent to the subscriber's circuit.

Default

No access control list is assigned.

Usage Guidelines

Use the **ip access-group** command to assign an IP access control list to packets associated with a context, an interface, or a subscriber's circuit.

An IP access control list that is applied to a context using the **ip access-group** command is called an administrative access control list. With this command, unauthorized access to the administration (for example, Telnet, Simple Management Network Protocol [SNMP], Internet Control Message Protocol [ICMP], and HTTP access) of the Subscriber Management System (SMS) device can be prevented.

The **ip access-group** command in interface configuration mode applies an access list to an interface, restricting the flow of traffic through the SMS device. Likewise, the **ip access-group** command in subscriber configuration mode applies an access list to a subscriber, restricting the flow of traffic through the SMS device.

Use the **ip access-list** command to create the access control list and enter access control list configuration mode where you can define conditions using the **permit**, **deny**, and **redirect** commands.

Use the **aaa authorization access-list** command to enable downloading of a remotely configured access list from a RADIUS server.

Use the **no** form of this command to remove an applied access control list from a context, interface, or subscriber record.

Examples

The following example applies the access control list called `WebCacheACL` to the subscriber named `topgun`:

```
[local]RedBack(config)#context fighter
[local]RedBack(config-ctx)#subscriber name topgun
[local]RedBack(config-sub)#ip access-group WebCacheACL out
```

Related Commands

aaa authorization access-list
ip access-group
ip access-list

ip access-list

ip access-list *list-name*

{**no** | **default**} **ip access-list** *list-name*

Purpose

Creates an IP access control list and enters access control list configuration mode.

Command Mode

context configuration

Syntax Description

list-name	Name of the access control list. Must be unique within the context.

Default

None

Usage Guidelines

Use the **ip access-list** command to create an access control list and enter access control list configuration mode where you can define conditions using the **permit** and **deny** commands.

Once the IP access control list is created and its conditions have been set, you can apply the list to a context, interface, or subscriber. An IP access control list that is applied to a context using the **ip access-group** context configuration command is called an administrative access control list, which prevents unauthorized access to the Subscriber Management System (SMS) device itself. The **ip access-group** command in interface configuration mode applies an access list to an interface or set of interfaces, restricting the flow of traffic through the SMS device. Likewise, the **ip access-group** command in subscriber configuration mode applies an access list to a subscriber or set of subscribers, restricting the flow of traffic through the SMS device.

Use the **no** or **default** form of this command to remove an applied access control list.

Examples

The following example creates an access list called `WebCacheACL`:

```
[local]RedBack(config-ctx)#ip access-list WebCacheACL
[local]RedBack(config-acl)#
```

Related Commands

ip access-group
{permit | deny}
redirect interface next-hop

ip dynamic-acl timeout

ip dynamic-acl timeout *seconds*

default ip dynamic-acl timeout

Purpose

Sets the amount of time an existing dynamic redirect is maintained once traffic has stopped flowing from the destination direction.

Command Mode

global configuration

Syntax Description

seconds	Number of seconds the dynamic redirect is to be maintained. The range of values is 0 to 600; the default value is 30.

Default

Dynamic redirects are maintained for 30 seconds after traffic has stopped flowing from the destination direction.

Usage Guidelines

Use the **ip dynamic-acl timeout** command to set the amount of time that a dynamic redirect is maintained once traffic has ceased in the destination direction. The destination direction of the dynamic redirect is the source of the original connection—the connection that triggered the redirection. Only traffic from that original source is monitored for purposes of beginning the countdown of the timeout period to prevent undesirable extension of the access to that port.

Use the **default** form of this command to return the timeout period to 30 seconds.

Examples

The following example sets the dynamic redirect timeout period higher than the default to accommodate a slow system:

```
[local]RedBack(config)#ip dynamic-acl timeout 100
```

Related Commands

redirect interface next-hop
show ip dynamic-acl subscriber

ip reflexive timeout

ip reflexive timeout *seconds*

default ip reflexive timeout

Purpose

Sets the amount of time an existing reflexive access control list is maintained once traffic has stopped flowing from the destination direction.

Command Mode

global configuration

Syntax Description

seconds	Number of seconds the reflexive access control list is to be maintained. The range of values is 0 to 600; the default value is 30.

Default

Reflexive access control lists are maintained for 30 seconds after traffic has stopped flowing from the destination direction.

Usage Guidelines

Use the **ip reflexive timeout** command to set the amount of time that a reflexive access control list is to be maintained once traffic has ceased in the destination direction. The destination direction of the reflexive access control list is the source of the original connection—the connection that triggered the reflexive access control list. Only traffic from that original source is monitored for purposes of beginning the countdown of the timeout period to prevent undesirable extension of the access to that port.

Use the **default** form of this command to return the reflexive timeout period to 30 seconds.

Examples

The following example sets the reflexive timeout period higher than the default in order to accommodate a slow system:

```
[local]RedBack(config)#ip reflexive timeout 45
```

Related Commands

ip access-group

{permit | deny}

{**permit** | **deny**} {*source* [*source-wildcard*] | **any** | **host** *source*}

before {**permit** | **deny**} {*source* [*source-wildcard*] | **any** | **host** *source*}

after {**permit | deny**} {*source* [*source-wildcard*] | **any** | **host** *source*}

no {**permit** | **deny**} {*source* [*source-wildcard*] | **any** | **host** *source*}

Purpose

Allows or prevents the passage of packets (any protocol) from the specified source or sources.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source IP address indicating that traffic originating from all IP addresses is to be included in the permit or deny criteria; identical to 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).

Default

None

Usage Guidelines

Use the {**permit** | **deny**} command to allow or prevent the flow of traffic (any protocol) from one or more IP addresses. Remember that there is an implicit **deny any** command at the end of every access control list.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all traffic originating from host `10.10.10.255` is to be denied access, and all others are to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny host 10.10.10.255
[local]RedBack(config-acl)#permit any
```

The following example specifies that all traffic originating from IP addresses beginning with `20.20` are to be denied access, and all others are to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny 20.20.0.0 0.0.255.255
[local]RedBack(config-acl)#permit any
```

Related Commands

ip access-group
ip access-list
{permit | deny} icmp
{permit | deny} igmp
{permit | deny} ip
{permit | deny} {tcp | udp}
redirect interface next-hop

{permit | deny} icmp

{**permit** | **deny**} **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

before {**permit** | **deny**} **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

after {**permit** | **deny**} **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

no {**permit** | **deny**} **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

Purpose

Allows or prevents the passage of Internet Control Message Protocol (ICMP) packets that meet the specified criteria.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source or destination IP address indicating that traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.

destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
***host** destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
icmp-type	Optional. A particular ICMP message type to be permitted or denied. The range of values is 0 to 255.
icmp-code	Optional if you use the *icmp-type* argument. A particular ICMP message code to be permitted or denied. The range of values is 0 to 255.

Default

None

Usage Guidelines

Use the {**permit** | **deny**} **icmp** command to allow or prevent the passage of ICMP packets matching the specified criteria. Remember that there is an implicit **deny any** command at the end of every access control list.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all ICMP echo request (ping request) traffic is to be dropped and all other traffic is to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny icmp any any 8 0
[local]RedBack(config-acl)#permit icmp any any
```

Related Commands

ip access-group
ip access-list
{permit | deny}
{permit | deny} igmp
{permit | deny} ip
{permit | deny} {tcp | udp}
redirect interface next-hop icmp

{permit | deny} igmp

{**permit** | **deny**} **igmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*igmp-type*]

before {**permit** | **deny**} **igmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*igmp-type*]

after {**permit** | **deny**} igmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destinatio*n} [*igmp-type*]

no {**permit** | **deny**} **igmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*igmp-type*]

Purpose

Allows or prevents the passage of Internet Group Management Protocol (IGMP) packets that meet the specified criteria.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source or destination IP address indicating that IGMP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.

destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
igmp-type	Optional. Type of IGMP packet to be matched. The range of values is decimal 0 to 255; the values can be expressed in either a decimal or hexadecimal format. Table 37-1 lists well-known and most commonly used types. Values listed in hexadecimal format must be prefaced with 0x. Numbers entered without the prefix are treated as decimal values.

Table 37-1 provides the hex and decimal values for common IGMP query types.

Table 37-1 IGMP Query Types and Values

IGMP Query Type Name	Hex Value	Decimal Value
Host Membership Query	0x11	17
Host Membership Report	0x12	18
DVMRP packets	0x13	19
IGMPv2 Membership Report	0x16	22
IGMPv2 Leave Group message	0x17	23
Multicast Traceroute response	0x1e	30
Multicast Traceroute query/request	0x1f	31
IGMPv3 Membership Report	0x1f	31

Default

None

Usage Guidelines

Use the {**permit** | **deny**} **igmp** command to allow or prevent the passage of IGMP packets matching the specified criteria. Remember that there is an implicit **deny any** command at the end of every access control list.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all multicast traceroute query/requests are to be denied, and all other types of IGMP traffic are to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny igmp any any 0x1f
[local]RedBack(config-acl)#permit any any
```

Related Commands

ip access-group
ip access-list
{permit | deny}
{permit | deny} icmp
{permit | deny} ip
{permit | deny} {tcp | udp}

{permit | deny} ip

{**permit** | **deny**} **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

before {**permit** | **deny**} **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

after {**permit** | **deny**} **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

no {**permit** | **deny**} **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

Purpose

Allows or prevents the passage of IP packets that meet the specified criteria.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.

host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).

Default

None

Usage Guidelines

Use the {**permit** | **deny**} **ip** command to allow or prevent the passage of IP packets matching the specified criteria. Remember that there is an implicit **deny any** command at the end of every access control list.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all IP traffic from subnet 10.25/16 is to be allowed. All other traffic is dropped because of the implicit **deny any** command at the end of the access control list:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#permit ip 10.25.0.0 0.0.255.255 any
```

The following example specifies that all IP traffic to destination host `10.25.1.1` is to be denied, and all other traffic on subnet 10.25.1/24 is to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny ip any host 10.25.1.1
[local]RedBack(config-acl)#permit ip any 10.25.1.0 0.0.0.255
```

Related Commands

ip access-group
ip access-list
{permit | deny}
{permit | deny} icmp
{permit | deny} igmp
{permit | deny} {tcp | udp}
redirect interface next-hop ip

{permit | deny} {tcp | udp}

{**permit** | **deny**} {**tcp** | **udp**} {*source source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** port | **neq** *port* | **range** *port endport*] [**established**]

before {**permit** | **deny**} {**tcp** | **udp**} {*source source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**]

after {**permit** | **deny**} {**tcp** | **udp**} {*source source-wildcard* | *any* | *host source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**]

no {**permit** | **deny**} {**tcp** | **udp**} {*source source-wildcard* | *any* | *host source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**]

Purpose

Allows or prevents the passage of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets that meet the specified criteria.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0. 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).

eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
destination	Destination address to be included in the deny criteria. Expressed as an IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
established	Optional. Specifies that only established connections are to be matched.

Default

None

Usage Guidelines

Use the {**permit** | **deny**} {**tcp** | **udp**} command to allow or prevent the passage of TCP or UDP packets matching the specified criteria. Remember that there is an implicit **deny any** command at the end of every access control list.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that FTP traffic is to be denied, and DNS traffic is to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny tcp any any eq 21
[local]RedBack(config-acl)#permit tcp any any eq 53
[local]RedBack(config-acl)#permit udp any any eq 53
```

The following example specifies that all TCP traffic to host `10.10.1.1` is to be denied, and TCP traffic to all other destinations on network `10.10.0.0` with `established` TCP connections is to be permitted:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny tcp any host 10.10.1.1
[local]RedBack(config-acl)#permit tcp any 10.10.0.0 0.0.255.255 established
```

Related Commands

ip access-group
ip access-list
{permit | deny}
{permit | deny} icmp
{permit | deny} igmp
{permit | deny} ip
redirect interface next-hop {tcp | udp}

redirect *interface next-hop*

redirect *interface next-hop* {*source* [*source-wildcard*] | **any** | **host** *source*} [**watch** *construct*]

before redirect *interface next-hop* {*source* [*source-wildcard*] | **any** | **host** *source*} [**watch** *construct*]

after redirect *interface next-hop* {*source* [*source-wildcard*] | **any** | **host** *source*} [**watch** *construct*]

no redirect *interface next-hop* {*source* [*source-wildcard*] | **any** | **host** *source*} [**watch** *construct*]

Purpose

Redirects packets (any protocol) matching the criteria to the specified next-hop IP address through the specified interface.

Command Mode

access control list configuration

Syntax Description

interface	Name of the interface through which packets matching the criteria are to be redirected.
next-hop	IP address in the form A.B.C.D to which packets matching the criteria are to be redirected.
source	Source address to be included in the redirect criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source IP address indicating that IP traffic to or from all IP addresses is to be included in the redirect criteria; identical to 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).

watch *construct*

Specifies that the access control list is to watch for traffic coming from the subscriber. If present, the redirect entry in the access control list does not become active until traffic from the subscriber matches that specified in the **watch** *construct*. The **watch** *construct* makes the access control list entry a redirect/watch entry. Any of the following syntax structures may be used for the **watch** *construct*:

watch {*source source-wildcard* | **any** | **host** *source*}

watch ip {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | *host destination*}

watch {**tcp** | **udp**} {*source source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** port | **neq** *port* | **range** *port endport*] [**established**]

watch igmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*igmp-type*]

watch icmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

Table 37-2 defines the individual syntax elements that can be used in the **watch** construct.

Table 37-2 Syntax Elements Possible in the watch Construct

source	Source address of traffic for which the dynamic redirect access control list entry is watching; an IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Completely wild-carded source IP address indicating that traffic originating from all IP addresses is to be included in the watch criteria; identical to 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address of traffic for which the dynamic redirect access control list entry is watching. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.

host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
established	Specifies that only established connections are to be matched.
igmp-type	Type of IGMP packet to be matched. The range of values is decimal 0 to 255; the values can be expressed in either decimal or hexadecimal. Well-known and most commonly used types are listed in Table 37-3. Values listed in hexadecimal must be prefaced with '0x'. Numbers entered without the prefix are treated as decimal values.
icmp-type	Optional. ICMP message type. The range of values is 0 to 255.
icmp-code	Optional if *icmp-type* is specified. ICMP message code. The range of values is 0 to 255.

Table 37-3 provides the hex and decimal values for common IGMP query types.

Table 37-3 IGMP Query Types and Values

IGMP Query Type Name	Hex Value	Decimal Value
Host Membership Query	0x11	17
Host Membership Report	0x12	18
DVMRP packets	0x13	19
IGMP v2 Membership Report	0x16	22
IGMPv2 Leave Group message	0x17	23
Multicast Traceroute response	0x1e	30
Multicast Traceroute query/request	0x1f	31
IGMPv3 Membership Report	0x1f	31

Default

None

Usage Guidelines

Use the **redirect** *interface next-hop* command to redirect packets matching the criteria to the specified next-hop IP address through the specified interface, regardless of any forwarding table information. Remember that there is an implicit **deny any** command at the end of every access control list.

If the command contains a **watch** *construct*, the entry created in the access control list is a redirect/watch entry, capable of creating a dynamic redirect that only takes effect when traffic matching the criteria specified in the **watch** *construct* is detected. At that time, traffic is redirected according to the instructions in the **redirect** command until the time period specified in the **ip dynamic-acl timeout** command has elapsed.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all traffic is to be redirected out to interface `atm501` using next-hop `10.1.1.2`:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect atm501 10.1.1.2 any
```

The following example specifies that all IP packets from host `10.1.1.10` are to be dropped, and all packets from subnet `10.1.1.0` are to be redirected to interface `enet0` via next-hop `20.1.1.2`. Packets from all other networks are dropped due to the implicit **deny any** command at the end of the access control list:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#deny ip host 10.1.1.10 any
[local]RedBack(config-acl)#redirect enet0 20.1.1.2 10.1.1.0 0.0.0.255
```

The following example includes a redirect/watch entry that creates a dynamic redirect when the criteria are met. All traffic is to be redirected out to interface `atm501` using next-hop `10.1.1.2`, but not unless traffic is detected from the subscriber that matches the criteria specified in the **watch** *construct*:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect atm501 10.1.1.2 any watch icmp host 1.1.1.10 host
172.20.1.2
```

Once traffic is detected that matches the criteria in the **watch** *construct*, all traffic is redirected out to interface `atm501` using next-hop `10.1.1.2` until the timeout period specified in the **ip dynamic-acl timeout** command has elapsed.

Related Commands

ip access-group
ip access-list
ip dynamic-acl timeout
{permit | deny}
redirect interface next-hop icmp
redirect interface next-hop ip
redirect interface next-hop {tcp | udp}
show ip dynamic-acl subscriber

redirect *interface next-hop* icmp

redirect *interface next-hop* **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]] [**watch** *construct*]

before redirect *interface next-hop* **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]] [**watch** *construct*]

after redirect *interface next-hop* **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*] [**watch** *construct*]

no redirect *interface next-hop* **icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]] [**watch** *construct*]

Purpose

Redirects Internet Control Message Protocol (ICMP) packets matching the criteria to the specified next-hop IP address through the specified interface.

Command Mode

access control list configuration

Syntax Description

interface	Name of the interface through which packets matching the criteria are to be redirected.
next-hop	IP address in the form A.B.C.D to which packets matching the criteria are to be redirected.
source	Source address to be included in the redirect criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the redirect criteria. Identical to 0.0.0.0 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address to be included in the redirect criteria. An IP address in the form A.B.C.D.

destination-wildcard — Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.

icmp-type — Optional. ICMP message type. The range of values is 0 to 255.

icmp-code — Optional if you use the *icmp-type* argument. ICMP message code. The range of values is 0 to 255.

watch *construct* — Specifies that the access control list is to watch for traffic coming from the subscriber. If present, the redirect entry in the access control list does not become active until traffic from the subscriber matches that specified in the **watch** *construct*. The **watch** *construct* makes the access control list entry a redirect/watch entry. Any of the following syntax structures may be used for the **watch** *construct*:

watch {*source source-wildcard* | **any** | **host** *source*}

watch ip {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | *host destination*}

watch {**tcp** | **udp**} {*source source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** port | **neq** *port* | **range** *port endport*] [**established**]

watch igmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*igmp-type*]

watch icmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

Table 37-4 defines the individual syntax elements that can be used in the **watch** construct.

Table 37-4 Syntax Elements Possible in the watch Construct

source — Source address of traffic for which the dynamic redirect access control list entry is watching; an IP address in the form A.B.C.D.

source-wildcard — Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.

any — Completely wild-carded source IP address indicating that traffic originating from all IP addresses is to be included in the watch criteria; identical to 255.255.255.255.

host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address of traffic for which the dynamic redirect access control list entry is watching. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
established	Specifies that only established connections are to be matched.
igmp-type	Optional. Type of IGMP packet to be matched. The range of values is decimal 0 to 255; the values can be expressed in either decimal or hexadecimal. Well-known and most commonly used types are listed in Table 37-3. Values listed in hexadecimal must be prefaced with '0x'. Numbers entered without the prefix are treated as decimal values.
icmp-type	Optional. ICMP message type. The range of values is 0 to 255.

icmp-code Optional if you use the *icmp-type* argument. ICMP message code. The range of values is 0 to 255.

Table 37-5 provides the hex and decimal values for common IGMP query types.

Table 37-5 IGMP Query Types and Values

IGMP Query Type Name	Hex Value	Decimal Value
Host Membership Query	0x11	17
Host Membership Report	0x12	18
DVMRP packets	0x13	19
IGMPv2 Membership Report	0x16	22
IGMPv2 Leave Group message	0x17	23
Multicast Traceroute response	0x1e	30
Multicast Traceroute query/request	0x1f	31
IGMPv3 Membership Report	0x1f	31

Default

None

Usage Guidelines

Use the **redirect** *interface next-hop* **icmp** command to redirect ICMP packets matching the criteria to the specified next-hop IP address through the specified interface, regardless of any forwarding table information. Remember that there is an implicit **deny any** at the end of every access control list.

If the command contains a **watch** *construct*, the entry created in the access control list is a redirect/watch entry, capable of creating a dynamic redirect that only takes effect when traffic matching the criteria specified in the **watch** *construct* is detected. At that time, traffic is redirected according to the instructions in the first part of the **redirect** command until the time period specified in the **ip dynamic-acl timeout** command has elapsed.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example redirects all ICMP traffic from host 60.168.10.35 to interface `atm1` via next-hop 21.175.83.165:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect atm1 21.175.83.165 icmp host 60.168.10.35 any
```

The following example redirects all ICMP traffic from host `60.168.10.35` to interface `atm2` via next-hop `21.175.83.165`, but not unless traffic is detected from the subscriber that matches the criteria specified in the **watch** *construct*:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect atm1 21.175.83.165 icmp host 60.168.10.35 any watch
icmp host 1.1.1.10 host 172.20.1.2
```

Once traffic is detected that matches the criteria in the **watch** *construct*, all traffic is redirected out to interface `atm2` using next-hop `21.175.83.165` until the timeout period specified in the **ip dynamic-acl timeout** command has elapsed.

Related Commands

ip access-group
ip access-list
ip dynamic-acl timeout
{permit | deny} icmp
redirect interface next-hop
redirect interface next-hop ip
redirect interface next-hop {tcp | udp}
show ip dynamic-acl subscriber

redirect *interface next-hop* ip

redirect *interface next-hop* **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [**watch** *construct*]

before redirect *interface next-hop* **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [**watch** *construct*]

after redirect *interface next-hop* **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [**watch** *construct*]

no redirect *interface next-hop* **ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [**watch** *construct*]

Purpose

Redirects IP packets matching the criteria to the specified *next-hop* IP address through the specified interface.

Command Mode

access control list configuration

Syntax Description

interface	Name of the interface through which packets matching the criteria are to be redirected.
next-hop	IP address in the form A.B.C.D to which packets matching the criteria are to be redirected.
source	Source address to be included in the redirect criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the redirect criteria. Identical to 0.0.0.0 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address to be included in the redirect criteria. An IP address in the form A.B.C.D.

destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
watch *construct*	Specifies that the access control list is to watch for traffic coming from the subscriber. If present, the redirect entry in the access control list does not become active until traffic from the subscriber matches that specified in the **watch** *construct*. The **watch** *construct* makes the access control list entry a redirect/watch entry. Any of the following syntax structures may be used for the **watch** *construct*: **watch** {*source source-wildcard* | **any** | **host** *source*} **watch ip** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} **watch** {**tcp** | **udp**} {*source source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* **|** **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** port | **neq** *port* **|** **range** *port endport*] [**established**] **watch igmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination}* [*igmp-type*] **watch icmp** {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]] Table 37-6 defines the individual syntax elements that can be used in the **watch** construct.

Table 37-6 Syntax Elements Possible in the watch Construct

source	Source address of traffic for which the dynamic redirect access control list entry is watching; an IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source IP address indicating that traffic originating from all IP addresses is to be included in the watch criteria; identical to 255.255.255.255.

host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address of traffic for which the dynamic redirect access control list entry is watching. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
established	Specifies that only established connections are to be matched.
igmp-type	Optional. Type of IGMP packet to be matched. The range of values is decimal 0 to 255; the values can be expressed in either decimal or hexadecimal format. Table 37-3 lists well-known and most commonly used types. Values listed in hexadecimal format must be prefaced with '0x'. Numbers entered without the prefix are treated as decimal values.
icmp-type	Optional. ICMP message type. The range of values is 0 to 255.

icmp-code Optional if you use the *icmp-type* argument. ICMP message code. The range of values is 0 to 255.

Table 37-7 provides the hex and decimal values for common IGMP query types.

Table 37-7 IGMP Query Types and Values

IGMP Query Type Name	Hex Value	Decimal Value
Host Membership Query	0x11	17
Host Membership Report	0x12	18
DVMRP packets	0x13	19
IGMPv2 Membership Report	0x16	22
IGMPv2 Leave Group message	0x17	23
Multicast Traceroute response	0x1e	30
Multicast Traceroute query/request	0x1f	31
IGMPv3 Membership Report	0x1f	31

Default

None

Usage Guidelines

Use the **redirect** *interface next-hop* **ip** command to redirect IP packets matching the criteria to the specified next-hop IP address through the specified interface, regardless of any forwarding table information. Remember that there is an implicit **deny any** command at the end of every access control list.

If the command contains a **watch** *construct*, the entry created in the access control list is a redirect/watch entry, capable of creating a dynamic redirect that only takes effect when traffic matching the criteria specified in the **watch** *construct* is detected. At that time, traffic is redirected according to the instructions in the first part of the **redirect** command until the time period specified in the **ip dynamic-acl timeout** command has elapsed.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example redirects all IP packets from host `138.1.174.71` to network `72.11.174.0` out to interface `atm3` via next-hop `21.177.86.104`:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect atm3 21.177.86.104 ip host 138.1.174.71 72.11.174.0
0.0.0.255
```

The following example redirects all IP packets from host `138.1.174.71` to network `72.11.174.0` out to interface `atm3` via next-hop `21.177.86.104`, but not unless traffic is detected from the subscriber that matches the criteria specified in the **watch** *construct*:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect atm3 21.177.86.104 ip host 138.1.174.71 72.11.174.0
0.0.0.255 watch icmp host 1.1.1.10 host 172.20.1.2
```

Once traffic is detected that matches the criteria in the **watch** *construct*, all traffic is redirected out to interface `atm3` using next-hop `21.177.86.104` until the timeout period specified in the **ip dynamic-acl timeout** command has elapsed.

Related Commands

ip access-group
ip access-list
ip dynamic-acl timeout
{permit | deny} ip
redirect interface next-hop
redirect interface next-hop icmp
redirect interface next-hop {tcp | udp}
show ip dynamic-acl subscriber

redirect *interface next-hop* {tcp | udp}

redirect *interface next-hop* {**tcp** | **udp**} {***source*** *source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**] [**watch** *construct*]

before redirect *interface next-hop* {**tcp** | **udp**} {***source*** *source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**] [**watch** *construct*]

after redirect *interface next-hop* {**tcp** | **udp**} {***source*** *source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**] [**watch** *construct*]

no redirect *interface next-hop* {**tcp** | **udp**} {***source*** *source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *port endport*] [**established**] [**watch** *construct*]

Purpose

Redirects Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets matching the criteria to the specified next-hop IP address through the specified interface.

Command Mode

access control list configuration

Syntax Description

interface	Name of the interface through which packets matching the criteria are to be redirected.
next-hop	IP address in the form A.B.C.D to which packets matching the criteria are to be redirected.
source	Source address to be included in the redirect criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.

any	Specifies a completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the redirect criteria. Identical to 0.0.0.0 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
destination	Destination address to be included in the redirect criteria. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
established	Specifies that only established connections are to be matched.

watch *construct*

Specifies that the access control list is to watch for traffic coming from the subscriber. If present, the redirect entry in the access control list does not become active until traffic from the subscriber matches that specified in the **watch** *construct*. The **watch** *construct* makes the access control list entry a redirect/watch entry. Any of the following syntax structures may be used for the **watch** *construct*:

watch {*source source-wildcard* | **any** | **host** *source*}

watch ip {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | *host destination*}

watch {**tcp** | **udp**} {*source source-wildcard* | **any** | **host** *source*} [**eq** *port* | **gt** *port* **|** **lt** *port* | **neq** *port* | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** *port* | **gt** *port* | **lt** port | **neq** *port* **|** **range** *port endport*] [**established**]

watch igmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination}* [*igmp-type*]

watch icmp {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*} [*icmp-type* [*icmp-code*]]

Table 37-8 defines the individual syntax elements that can be used in the **watch** construct.

Table 37-8 Syntax Elements Possible in the watch Construct

source	Source address of traffic for which the dynamic redirect access control list entry is watching; an IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Completely wild-carded source IP address indicating that traffic originating from all IP addresses is to be included in the watch criteria; identical to 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address of traffic for which the dynamic redirect access control list entry is watching. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.

host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).
eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port,* and **range** *port endport* constructs are mutually exclusive.
established	Specifies that only established connections are to be matched.
igmp-type	Optional. Type of IGMP packet to be matched. The range of values is decimal 0 to 255; the values can be expressed in either decimal or hexadecimal format. Table 37-3 lists well-known and most commonly used types.Values listed in hexadecimal format must be prefaced with '0x'. Numbers entered without the prefix are treated as decimal values.
icmp-type	Optional. ICMP message type. The range of values is 0 to 255.
icmp-code	Optional if you use the *icmp-type* argument. ICMP message code. The range of values is 0 to 255.

Table 37-9 provides the hex and decimal values for common IGMP query types.

Table 37-9 IGMP Query Types and Values

IGMP Query Type Name	Hex Value	Decimal Value
Host Membership Query	0x11	17
Host Membership Report	0x12	18
DVMRP packets	0x13	19
IGMPv2 Membership Report	0x16	22
IGMPv2 Leave Group message	0x17	23
Multicast Traceroute response	0x1e	30
Multicast Traceroute query/request	0x1f	31
IGMPv3 Membership Report	0x1f	31

Default

None

Usage Guidelines

Use the **redirect** *interface next-hop* {**tcp** | **udp**} command to redirect TCP or UDP packets matching the criteria to the specified next-hop IP address through the specified interface, regardless of any forwarding table information. Remember that there is an implicit **deny any** at the end of every access control list.

If the command contains a **watch** *construct*, the entry created in the access control list is a redirect/watch entry, capable of creating a dynamic redirect that only takes effect when traffic matching the criteria specified in the **watch** *construct* is detected. At that time, traffic is redirected according to the instructions in the first part of the **redirect** command until the time period specified in the **ip dynamic-acl timeout** command has elapsed.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example redirects all HTTP (TCP port 80) traffic to interface `enet1` via next-hop `177.138.1.19`:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect enet1 177.138.1.19 tcp any any eq 80
```

The following example redirects all HTTP (TCP port 80) traffic to interface `enet1` via next-hop `177.138.1.19`, but not unless traffic is detected from the subscriber that matches the criteria specified in the **watch** *construct*:

```
[local]RedBack(config-ctx)#ip access-list protect201
[local]RedBack(config-acl)#redirect enet1 177.138.1.19 tcp any any eq 80 watch icmp
host 1.1.1.10 host 172.20.1.2
```

Once traffic is detected that matches the criteria in the **watch** *construct*, all traffic is redirected out to interface `enet1` using next-hop `177.138.1.19` until the timeout period specified in the **ip dynamic-acl timeout** command has elapsed.

Related Commands

ip access-group
ip access-list
ip dynamic-acl timeout
{permit | deny} {tcp | udp}
redirect interface next-hop
redirect interface next-hop icmp
redirect interface next-hop ip
show ip dynamic-acl subscriber

reflexive {ftp | tftp}

reflexive {**ftp** | **tftp**} {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

before reflexive {**ftp** | **tftp**} {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

after reflexive {**ftp** | **tftp**} {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

no reflexive {**ftp** | **tftp**} {*source source-wildcard* | **any** | **host** *source*} {*destination destination-wildcard* | **any** | **host** *destination*}

Purpose

Defines criteria for a reflexive access control list for either File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) using the standard port numbers for those protocols.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
any	Specifies a completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0. 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
destination	Destination address to be included in the deny criteria. An IP address in the form A.B.C.D.

destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).

Default

None

Usage Guidelines

Use the **reflexive** {**ftp** | **tftp**} command to enable the stateful firewall (reflexive access control list) feature and to define the criteria that must be matched to install a reflexive access control list for FTP or TFTP.

With a reflexive access control list, traffic is watched in one direction to see if the configured criteria are matched. If the criteria are matched, then a reflexive access control list is dynamically installed for the return trip traffic. Since the port numbers are standard for FTP and TFTP, they do not need to be explicitly specified in this command. The reflexive access control list exists solely for the session that matched the configured criteria. This is what is meant by the term *stateful*. When the session that matched the original criteria ends, the reflexive access control list is removed.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following FTP example specifies that Transmission Control Protocol (TCP) traffic to any host with a destination port number of 21 is to allow TCP connections only from the destination host to the source host if the source port is 20. The port numbers are not explicitly specified in the command because they are standard for FTP.

```
[local]RedBack(config-ctx)#ip access-list galaxy
[local]RedBack(config-acl)#permit tcp any any established
[local]RedBack(config-acl)#reflexive ftp any any
```

The **permit tcp any any established** entry in the access control list is necessary to allow established TCP connections back to the host.

Related Commands

ip access-group
ip access-list
reflexive {tcp | udp}

reflexive {tcp | udp}

reflexive {**tcp** | **udp**} {*source* [*source-wildcard*] | **any** | **host** *source*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] [**watch** {**dest-port eq** *port* | **source-port eq** *port* | **dest-port eq** *port* **source-port eq** *port*}]

before reflexive {**tcp** | **udp**} {*source* [*source-wildcard*] | **any** | **host** *source*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] [**watch** {**dest-port eq** *port* | **source-port eq** *port* | **dest-port eq** *port* **source-port eq** *port*}]

after reflexive {**tcp** | **udp**} {*source* [*source-wildcard*] | **any** | **host** *source*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] [**watch** {**dest-port eq** *port* | **source-port eq** *port* | **dest-port eq** *port* **source-port eq** *port*}]

no reflexive {**tcp** | **udp**} {*source* [*source-wildcard*] | **any** | **host** *source*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] {*destination destination-wildcard* | **any** | **host** *destination*} [**eq** {*port* | **learned**} | **gt** {*port* | **learned**} | **lt** {*port* | **learned**} | **neq** {*port* | **learned**} | **range** *port endport*] [**watch** {**dest-port eq** *port* | **source-port eq** *port* | **dest-port eq** *port* **source-port eq** *port*}]

Purpose

Defines the traffic to be watched in one direction to determine if traffic in the opposite direction should be allowed to pass.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. An IP address in the form A.B.C.D.
source-wildcard	Optional. Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.

any	Completely wild-carded source or destination IP address indicating that IP traffic to or from all IP addresses is to be included in the permit or deny criteria. Identical to 0.0.0.0. 255.255.255.255.
host *source*	Address of a single-host source with no wild-carded address bits. The **host** *source* construct is identical to the *source source-wildcard* construct if the wildcard address indicates that all bits should be matched (0.0.0.0).
eq *port*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
gt *port*	Optional. Specific source or destination port. The **gt** keyword indicates that a packet's port must be greater than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
lt *port*	Optional. Specific source or destination port. The **lt** keyword indicates that a packet's port must be less than the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
neq *port*	Optional. Specific source or destination port. The **neq** keyword indicates that a packet's port must not be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
learned	Optional. Beginning and ending source or destination ports that define a range of port numbers. A packet's port must fall within the specified range to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
range *port endport*	Optional. Specific source or destination port. The **eq** keyword indicates that a packet's port must be equal to the value specified in the *port* argument to match the criteria. The **eq** *port*, **gt** *port*, **lt** *port*, **neq** *port*, and **range** *port endport* constructs are mutually exclusive.
destination	Destination address to be included in the deny criteria. An IP address in the form A.B.C.D.
destination-wildcard	Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 32-bit quantity in a 4-byte dotted-decimal format. Zero-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument must match; one-bits in the *destination-wildcard* argument mean that the corresponding bits in the *destination* argument are ignored.
host *destination*	Address of a single-host destination with no wild-carded address bits. The **host** *destination* construct is identical to the *destination destination-wildcard* construct, if the wildcard address indicates that all bits should be matched (0.0.0.0).

watch	Optional. Specifies which destination and/or source port to look for. If a destination or source port is not specified, the inverse of the reflexive entry is assumed.
dest-port eq *port*	Optional. Specific destination port number to watch in one direction. If the destination port number matches, a dynamic entry is created for traffic in the other direction.
source-port eq *port*	Optional. Specific source port number to watch in one direction. If the source port number matches, a dynamic entry is created for traffic in the other direction.

Default

None

Usage Guidelines

Use the **reflexive** {**tcp** | **udp**} command to enable the stateful firewall (reflexive access control list) feature. This command defines the criteria that must be matched to install a reflexive access control list.

With a reflexive access control list, traffic is watched in one direction to see if the configured criteria are matched. If the criteria are matched, then a reflexive access control list is dynamically installed for the return trip traffic. This reflexive access control list exists solely for the session that matched the configured criteria. This is what is meant by the term *stateful*. When the session that matched the original criteria ends, the reflexive access control list is removed.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following File Transfer Protocol (FTP) example specifies that Transmission Control Protocol (TCP) traffic to any host with a destination port number of `21` is to allow TCP connections only from the destination host to the source host if the source port is `20`:

```
[local]RedBack(config-ctx)#ip access-list galaxy
[local]RedBack(config-acl)#permit tcp any any established
[local]RedBack(config-acl)#reflexive tcp any eq 20 any watch dest-port
eq 21
```

The **permit tcp any any established** entry in the access control list is necessary to allow established TCP connections back to the host.

Note This same access control could be accomplished using the **reflexive ftp** command without having to specify the port numbers because they are standard for FTP. See the **reflexive** {**ftp** | **tftp**} command description for more information.

Related Commands

ip access-group
ip access-list
reflexive {ftp | tftp}

show ip access-list

show ip access-list [*list-name*]

Purpose

Displays the indicated access list and the number of matches for each entry in the list.

Command Mode

administrator exec

Syntax Description

list-name	Optional. Name of a specific access list to be displayed.

Default

None

Usage Guidelines

Use the **show ip access-list** command to display the indicated access list and the number of matches for each entry in the list. If the *list-name* argument is omitted, a summary of all lists is displayed. Access control lists that were loaded from a Remote Authentication Dial-In User Service (RADIUS) server are indicated in the display with the word “downloaded.”

Examples

The following example displays the access control lists defined in the context called `blue`:

```
[local]RedBack#context blue
[blue]RedBack#show ip access-list

IP access list 101
 redirect radius 155.53.197.100 tcp any any eq 80
 permit tcp any any
 permit ip any any

IP access list 201 (downloaded)
 permit udp any host 10.10.20.30
 deny tcp any any
```

The following example names a specific access control list. The output indicates the number of matches for each entry in the access list. When there have been no matches, no number is indicated in parentheses:

```
[blue]RedBack#show ip access-list 101

IP access list 101
 redirect radius 155.53.197.100 tcp any any eq 80 (13 matches)
 permit tcp any any (1359 matches)
 permit ip any any (1970 matches)
```

Related Commands

aaa authorization access-list
ip access-group
ip access-list

show ip dynamic-acl subscriber

show ip dynamic-acl subscriber *sub-name*

Purpose

Displays the redirect/watch entries that are currently active for a specific subscriber.

Command Mode

administrator exec

Syntax Description

sub-name	Name of the subscriber for whom you want information displayed. The name must be in the default structured username format (*name*@context) or other configured custom format.

Default

None

Usage Guidelines

Use the **show ip dynamic-acl subscriber** command to show the redirect/watch entries that are currently active for a specific subscriber. An entry is considered active when traffic matches the criteria defined by the **watch** *construct* in a **redirect** command. Until there is traffic that matches those criteria, the redirect/watch entry is considered passive.

Examples

The following example uses the **show ip dynamic-acl subscriber** command to display the redirect/watch entries currently active for a subscriber named `joanna@corporate`:

```
[local]RedBack#show ip dynamic-acl subscriber joanna@corporate

SUBSCRIBER=joanna@corporate CONTEXT=corporate ACCESS-LIST=exec (out bound)
-------------------------------------------------------------------------------
redirect eth61 172.16.38.10 icmp host 172.20.1.2 host 1.1.1.10 watch icmp host 1.1.1.10
host 172.20.1.2 (141 matches) ttl=22s
-------------------------------------------------------------------------------
```

- `(141 matches)` indicates the number of matches the redirect/watch entry has logged.
- `ttl=22s` indicates the number of seconds before this dynamic redirect access control entry terminates.

Related Commands

ip dynamic-acl timeout

show ip reflexive-acl

show ip reflexive-acl subscriber *sub-name*

Purpose

Displays a list of reflexive access entries for the specified subscriber.

Command Mode

administrator exec

Syntax Description

subscriber *sub-name*	Alphanumeric string that identifies an active subscriber.

Default

None

Usage Guidelines

Use the **show ip reflexive-acl** command to display the reflexive access control lists that are in place for the named subscriber. The output contains both the reflexive access control lists as configured and the corresponding dynamic access control lists. The number of matches for each is also included in the display.

Examples

The following example displays dynamic access entries for a subscriber named `joe@local`:

```
[local]Redback#show ip reflexive-acl subscriber joe@local

SUBSCRIBER=joe@local CONTEXT=local ACCESS-LIST:trueblue (out bound)
------------------------------------------------------------------------------
reflexive ftp any any (34401 matches)
  permit tcp host 200.1.1.2 eq 20 host 200.1.2.2 gt 1024 (3270 matches) ttl=20s
------------------------------------------------------------------------------
FLOWS USED=1   AVAILABLE=19   MAX=20   TTL INTERVAL=30s
```

- `reflexive ftp any any` is the access control entry that was configured through the command-line interface (CLI).
- `(34401 matches)` indicates the number of matches the reflexive entry has logged.
- `permit tcp host 200.1.1.2 eq 20 host 200.1.2.2 gt 1024` is the dynamic access control entry that was created in response to the reflexive entry.

- `(3270 matches)` indicates the number of matches the dynamic entry has logged.
- `ttl=20s` indicates the number of seconds before this dynamic access control entry terminates.
- `FLOWS USED` indicates the number of dynamic access entries created.
- `AVAILABLE` indicates the number of dynamic access entries this subscriber can create.
- `MAX` indicates the total number of flows this subscriber can have active at any one time.
- `TTL INTERVAL` is the maximum time a flow can be sustained without any traffic before it is removed.

Related Commands

show ip access-list

Bridge Access Control List Commands

This chapter describes the commands related to building and editing bridge access control lists on a Redback system. An access control list is a series of statements that define the criteria used to determine whether a packet should be allowed to pass. Use the **bridge access-list** context configuration mode command to enter access control list configuration mode. This command requires the name of a new or existing access control list. All subsequent access control list configuration commands are applied to the access list you specify when you enter the mode.

Each access control list configuration command creates a statement in the access control list. When the access control list is applied (to a subscriber or to an interface), the action performed by each statement is one of the following:

- A **deny** statement causes any packet matching the criteria to be dropped.
- A **permit** statement causes any packet matching the criteria to be accepted.

All access control lists have an implicit **deny any** command at the end. A packet that does not match the criteria of the first statement is subjected to the criteria of the second statement, and so on, until the end of the access control list is reached; at which point, the packet is dropped.

When used without a prefix, each **deny** or **permit** command creates a new statement in the access control list. When used with the **before**, **after**, or **no** prefix, each command identifies an existing statement in the access control list.

The **before** and **after** prefixes are positioning prefixes. They indicate where in the access control list you want to insert additional statements. For example, if your access control list already consists of five statements and you want to insert more statements between the third and fourth, you would first use the **after** prefix, specifying the third statement (or the **before** prefix, specifying the fourth statement). The next new statement you create is then inserted between the original third and fourth statements. The next new statement is inserted after that one, and so on, until you provide a different positioning command. Without the instruction provided by a positioning command, each new statement you create is appended after the statement you created before it. Without any positioning commands at all, each new statement is appended to the end of the access control list.

Use the **bridge-group** command to apply a bridge access control list to an interface (in interface configuration mode), or a subscriber (in subscriber configuration mode). Use the **bind session** command to apply a bridge access control list to an Ethernet over Layer 2 Tunneling Protocol (L2TP) tunnel session. This is used to limit the traffic to Point-to-Point Protocol over Ethernet (PPPoE).

The **no** form of an access control list configuration command identifies and removes an individual statement from the access control list. To delete an entire access control list, enter context configuration mode, and use the **no** form of the **bridge access-list** command, naming the access list to be deleted. To disassociate an access list from the interface or subscriber to which it was applied, enter the appropriate mode, and use the **no** form of the **bridge-group** command.

For overview information, a description of the tasks used to configure bridge access control list features, and configuration examples, see the "Configuring Bridge Access Control Lists" chapter in the *Redback Access Operating System (AOS) Configuration Guide*.

access-list undefined

access-list undefined {**permit-all** | **deny-all**}

default access-list undefined

Purpose

Specifies how packets are to be handled (forwarded or dropped) when an undefined access control list is applied to a subscriber or to an interface within a context.

Command Mode

context configuration

Syntax Description

permit-all	Specifies that all packets should be forwarded when an undefined access control list has been applied to a subscriber or interface.
deny-all	Specifies that all packets should be dropped when an undefined access control list has been applied to a subscriber or interface.

Default

All packets are permitted.

Usage Guidelines

Use the **access-list undefined** command to specify how packets are to be handled when an undefined access control list is encountered. It is helpful to have this command in the configuration in cases where an access control list that has not yet been configured is applied to an interface or subscriber, or in cases where an incorrectly named access control list is applied. You can determine whether traffic intended for the interface or subscriber in such an instance is forwarded or dropped. Once a defined access control list is applied to the interface or subscriber, traffic can be transmitted according to the parameters of that access control list.

Use the **bridge access-list** command in subscriber or interface configuration mode to create an access control list. Use the **bridge-group** command in interface configuration mode to apply the access control list to an interface. Use the **bridge-group** command in subscriber configuration mode to apply the access control list to a subscriber.

Use the **default** form of this command to specify that all packets are to be forwarded when an undefined access control list has been applied to a subscriber or interface.

Examples

The following example sets the **access-list undefined** command to `deny-all` for the `local` context and defines an access control list called `access-list-1100`:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#access-list undefined deny-all
[local]RedBack(config-ctx)#bridge access-list-1100
[local]RedBack(config-acl)#permit 01:00:5e:00:00:00 00:00:00:ff:ff:ff
```

The following example shows that the administrator, intending to apply the access control list called `access-list-1100` to the subscriber named `joe`, inadvertently types the name as `access-list-1000`:

```
[local]RedBack(config-ctx)#subscriber name joe
[local]RedBack(config-sub)#bridge-group trinity access-group access-list-1000 out
```

The result is that packets intended for the subscriber are dropped. If the **access-list undefined** command had been omitted (or used the **permit-all** keyword), all packets would have been forwarded.

Related Commands

bridge access-list
bridge-group

bridge access-list

bridge access-list *list-name*

no bridge access-list *list-name*

Purpose

Creates a bridge access control list and enters access control list configuration mode.

Command Mode

context configuration

Syntax Description

list-name	Name of the access list. Must be unique within a context.

Default

None

Usage Guidelines

Use the **bridge access-list** command to create an access control list and enter access control list configuration mode where you can define conditions using the **permit** and **deny** commands.

Once the bridge access control list is created and its conditions have been set, you can apply the list to an interface using the **bridge-group** command in interface configuration mode, or indirectly to a circuit through a subscriber record using the **bridge-group** command in subscriber configuration mode.

Use the **no** form of this command to remove a named bridge access control list.

Examples

The following example creates a bridge access control list named `103`:

```
[local]RedBack(config-ctx)#bridge access-list 103
[local]RedBack(config-acl)#
```

Related Commands

bridge-group
{permit | deny}

bridge-group

bridge-group *group-name* [**aging-time** *time* | **path-cost** *cost* | **spanning-disabled** | **trans-bpdu** | **access-group** *group-name* {**in** | **out**}]

no bridge-group *group-name*

Purpose

Attaches an interface or a subscriber to a previously defined bridge group and allows specification of the bridge access control list to be applied.

Command Mode

interface configuration
subscriber configuration

Syntax Description

group-name	Alphanumeric string specifying the previously configured bridge group to which this interface or subscriber is to be attached.
aging-time *time*	Optional. Address age time, in seconds, for the particular circuit that will be bound to this interface or subscriber. This represents the aging of the learned Media Access Control (MAC) addresses. The range of values is 60 to 1,000,000; the default is 300.
path-cost *cost*	Optional. Path cost to the designated bridge. The total root path cost becomes the cost to the designated bridge plus the cost to root from the designated bridge. The range of values is 1 to 65,535; the default is 1.
spanning-disabled	Optional. Disables the IEEE 802.1D Spanning Tree Protocol for the particular circuit that will be bound to this interface or subscriber.
trans-bpdu	Optional. Causes the AOS to send spanning-tree bridge protocol data units (BPDUs) in transparent BPDU mode; that is, encapsulated within an 802.3 header using the Ethernet Logical Link Control (LLC) Subnetwork Access Protocol (SNAP) value. By default, spanning tree BPDUs are encapsulated as specified in RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, and RFC 1490, *Multiprotocol Interconnect over Frame Relay,* with their own LLC SNAP values.
access-group *group-name*	Optional. Name of a bridge access control list to be attached to the subscriber's circuit or applied to the interface.
in	Applies the bridge access control list to packets received by the subscriber's circuit or by the interface.
out	Applies the bridge access control list to packets sent by the subscriber's circuit or by the interface.

Default

The aging time is 300 seconds, the path cost is 1 unit, and the Spanning Tree Protocol is enabled.

Usage Guidelines

Use the **bridge-group** command in interface configuration mode to attach a bridge group to an interface. Use this command in subscriber configuration mode to attach a bridge group to a subscriber record. In either case, use the **access-group** *name* {**in** | **out**} construct to specify a bridge access control list to be applied to inbound or outbound traffic.

Use the **no** form of this command to disassociate the indicated bridge group from the interface or subscriber record.

Examples

The following example attaches the bridge group `redback-customers` to an interface called `enet1` and applies a bridge access control list called `no_non_customers` to all inbound traffic:

```
[local]RedBack(config-ctx)#bridge redback-customers
[local]RedBack(config-bridge)#exit
[local]RedBack(config-ctx)#subscriber name thomas
[local]RedBack(config-sub)#bridge-group redback-customers access-group no_non_customers
```

Related Commands

bridge access-list
show bridge access-list

{permit | deny}

{**permit** | **deny**} *source* [*source-wildcard* [*destination* [*destination-wildcard*]]] [[**lsap** *lsap* [*lsap-wildcard*]] | [**type** *type* [*type-wildcard*]]]

before {**permit** | **deny**} *source* [*source-wildcard* [*destination* [*destination-wildcard*]]] [[**lsap** *lsap* [*lsap-wildcard*]] | [**type** *type* [*type-wildcard*]]]

after {**permit** | **deny**} *source* [*source-wildcard* [*destination* [*destination-wildcard*]]] [[**lsap** *lsap* [*lsap-wildcard*]] | [**type** *type* [*type-wildcard*]]]

no {**permit** | **deny**} *source* [*source-wildcard* [*destination* [*destination-wildcard*]]] [[**lsap** *lsap* [*lsap-wildcard*]] | [**type** *type* [*type-wildcard*]]]

Purpose

Allows or prevents the passage of packets from the specified source or sources.

Command Mode

access control list configuration

Syntax Description

source	Source address to be included in the permit or deny criteria. A 48-bit Media Access Control (MAC) address in the form *hh:hh:hh:hh:hh:hh*, where *hh* is a hexadecimal number.
source-wildcard	Optional. Indication of which bits in the *source* argument are significant for purposes of matching. Expressed as a 48-bit MAC address in the form *hh:hh:hh:hh:hh:hh*, where *hh* is a hexadecimal number. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.
destination	Optional if a *source-wildcard* argument is specified. Destination address to be included in the permit or deny criteria. A 48-bit MAC address in the form *hh:hh:hh:hh:hh:hh*, where *hh* is a hexadecimal number.
destination-wildcard	Optional if a *destination* argument is specified. Indication of which bits in the *destination* argument are significant for purposes of matching. Expressed as a 48-bit MAC address in the form *hh:hh:hh:hh:hh:hh*, where *hh* is a hexadecimal number. Zero-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument must match; one-bits in the *source-wildcard* argument mean that the corresponding bits in the *source* argument are ignored.

lsap *lsap*	Optional. Link service access point (LSAP) to be included in the permit or deny criteria. Hexadecimal number in the range 0 through ffff, preceded by "0x" to indicate that a hex value follows.
lsap-wildcard	Optional if you use the **lsap** *lsap* construct. 16-bit hexadecimal number whose one-bits correspond to bits in the *lsap* argument that should be ignored when making a comparison. A mask for a destination service access point (DSAP) and source service access point (SSAP) pair should always be at least 0x0101, because these two bits are used for purposes other than identifying the service access point (SAP) codes.
type *type*	Optional. Ethertype or Subnetwork Access Protocol (SNAP) bytes that identify packets to be included in the permit or deny criteria. Hexadecimal number in the range 0 through ffff, preceded by "0x" to indicate that a hex value follows.
type-wildcard	Optional if you use the **type** *type* construct. 16-bit hexadecimal number whose one-bits correspond to bits in the type argument that should be ignored when making a comparison.

Default

None

Usage Guidelines

Use the {**permit** | **deny**} command to allow or prevent the flow of traffic from one or a range of MAC addresses. Additional keywords and arguments are available to narrow down the criteria further. Access control lists utilizing the **type** *type* construct can have significant impact on system performance. To minimize this effect, do not make lists any longer than necessary, and use wildcard bit masks whenever possible.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all packets coming from MAC address `01:00:5e:00:00:00` with Ethertype `0x800` are to be denied access:

```
[local]RedBack(config-ctx)#bridge access-list protect101
[local]RedBack(config-acl)#deny 01:00:5e:00:00:00 type 0x800
```

Related Commands

bridge access-list
bridge-group
{permit | deny} lsap
{permit | deny} type

{permit | deny} lsap

{**permit** | **deny**} **lsap** *lsap* [*lsap-wildcard*]

before {**permit** | **deny**} **lsap** *lsap* [*lsap-wildcard*]

after {**permit** | **deny**} **lsap** *lsap* [*lsap-wildcard*]

no {**permit** | **deny**} **lsap** *lsap* [*lsap-wildcard*]

Purpose

Allows or prevents the passage of packets matching the specified link service access point (LSAP) criteria.

Command Mode

access control list configuration

Syntax Description

lsap	Link service access point to be included in the permit or deny criteria. Hexadecimal number in the range 0 through ffff, preceded by 0x to indicate that a hex value follows.
lsap-wildcard	Optional. 16-bit hexadecimal number whose one-bits correspond to bits in the *lsap* argument that should be ignored when making a comparison. A mask for a destination service access point (DSAP) and source service access point (SSAP) pair should always be a least 0x0101, because these two bits are used for purposes other than identifying the service access point (SAP) codes.

Default

None

Usage Guidelines

Use the {**permit** | **deny**} **lsap** command to allow or prevent the flow of traffic from one or a range of LSAPs.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all packets coming from the `0xf0f0` LSAP (NetBIOS) are to be denied access, and all others are to be permitted:

```
[local]RedBack(config-ctx)#bridge access-list protect101
[local]RedBack(config-acl)#deny lsap 0xf0f0 0x0101
[local]RedBack(config-acl)#permit lsap 0x0000 0xffff
```

Related Commands

bridge access-list
bridge-group
{permit | deny}
{permit | deny} type

{permit | deny} type

{**permit** | **deny**} **type** *type* [*type-wildcard*]

before {**permit** | **deny**} **type** *type* [*type-wildcard*]

after {**permit** | **deny**} **type** *type* [*type-wildcard*]

no {**permit** | **deny**} **type** *type* [*type-wildcard*]

Purpose

Allows or prevents the passage of Ethernet type code packets matching the specified Ethernet Type II- or Ethernet Logical Link Control (LLC) Subnetwork Access Protocol (SNAP)-encapsulated packet criteria.

Command Mode

access control list configuration

Syntax Description

type	Ethertype code that identifies packets to be included in the permit or deny criteria. Hexadecimal number in the range 0 through ffff, preceded by 0x to indicate that a hex value follows.
type-wildcard	Optional. 16-bit hexadecimal number whose one-bits correspond to bits in the type argument that should be ignored when making a comparison.

Default

None

Usage Guidelines

Use the {**permit** | **deny**} **type** command to allow or prevent the flow of traffic from one or a range of Ethertype codes. Access control lists utilizing the **type** *type* construct can have significant impact on system performance. To minimize this effect, do not make lists any longer than necessary, and use wildcard bit masks whenever possible.

Use the **before** form of this command to specify an existing statement in the access control list before which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access control list after which you want to insert the next new statement that you create. All new statements then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access control list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example specifies that all packets coming from Ethertypes `0x800` through `0x8ff` are to be denied access, and all others are to be permitted:

```
[local]RedBack(config-ctx)#bridge access-list protect101
[local]RedBack(config-acl)#deny type 0x800 0x8ff
[local]RedBack(config-acl)#permit type 0x0000 0xffff
```

Related Commands

bridge access-list
bridge-group
{permit | deny}
{permit | deny} lsap

show bridge access-list

show bridge access-list [*list-name*]

Purpose

Displays one or all bridge access control lists in a context and the number of matches for each entry in each list.

Command Mode

administrator exec

Syntax Description

list-name	Optional. Name of a specific access control list to be displayed.

Default

Displays summary information for all bridge access control lists in the current context.

Usage Guidelines

Use the **show bridge access-list** command to display one or all bridge access control lists in a context and the number of matches for each entry in each list. If you do not use the optional *list-name* argument, this command displays all the bridge access control lists in the current context. If you specify a particular access control list, the resulting display includes only information about that access control list. In both cases, the number of matches for each entry in the list is shown unless the number of matches is zero (see examples below).

Examples

The following example shows how to display all bridge access control lists configured under the `cr1` context:

```
[cr1]Redback#show bridge access-list

Bridge access list abc
deny ff:ff:ff:ff:ff:ff 00:00:00:00:00:00 (12 matches)
permit 11:22:33:44:55:66 00:00:00:00:00:00 (27 matches)

Bridge access list ABC
deny ff:ff:ff:ff:ff:ff 00:00:00:00:00:00 (2 matches)
```

The following example shows how to display information for a specific access control list. When there are no matches for an entry in the list, no number in parenthesis appears following the entry.

```
[local]Redback#show bridge access-list brmac1

Bridge access list brmac1
permit 01:00:5e:00:00:00 00:00:00:ff:ff:ff (10 matches)
permit 11:22:33:44:55:66 00:00:00:00:00:00
```

Related Commands

bridge access-list
bridge-group

Service Access List Commands

This chapter describes the commands related to building and editing service access lists on a Redback system. A service access list is a series of statements that defines the criteria used to determine whether contexts, domains, and tunnels should be available to subscribers on a per-circuit basis. The **service access-list** command in global configuration mode is used to enter service access list configuration mode. This command requires the name of a new or existing service access list. All subsequent service access list configuration commands are applied to the access list you specify when you enter the mode.

Each service access list configuration command creates a statement in the access list. When the access list is applied (to a circuit, a port, an L2TP peer, or an L2F peer), the action performed by each statement is one of the following:

- A **deny** statement causes any service matching the criteria to be blocked.
- A **permit** statement causes any service matching the criteria to be allowed.

All service access lists have an implicit **deny any** command at the end. A service that does not match the criteria of the first statement is subjected to the criteria of the second statement, and so on, until the end of the access list is reached; at which point, the service is denied.

When used without a prefix, each **deny** or **permit** command creates a new statement in the access list. When used with the **before**, **after**, or **no** prefix, each command identifies an existing statement in the access list.

The **before** and **after** prefixes are positioning prefixes. They indicate where in the access list you want to insert additional statements. For example, if your access list already consists of five statements and you want to insert more statements between the third and fourth, you would first use the **after** prefix, specifying the third statement (or the **before** prefix, specifying the fourth statement). The next new statement you create is then inserted between the original third and fourth statements. The next new statement is inserted after that one, and so on, until you provide a different positioning command. Without the instruction provided by a positioning command, each new statement you create is appended after the statement you created before it. Without any positioning commands at all, each new statement is appended to the end of the service access list.

The **no** form of a service access list configuration command identifies and removes an individual statement from the access list. To delete an entire service access list, you would have to enter global configuration mode and use the **no** form of the **service access-list** command, naming the access list to be deleted. To disassociate a service access list from the circuit, port, or tunnel to which it was applied, you would have to enter the appropriate mode, and use the **no** form of either the **bind authentication** command, **session-auth** command in L2TP configuration mode, or **session-auth** command in L2F configuration mode, naming the service list in the optional **service-group** *name* construct.

For overview information, a description of the tasks used to configure service access list features, and configuration examples, see the "Configuring Service Access Lists" chapter in the *Access Operating System (AOS) Configuration Guide*.

{permit | deny} any

{permit | deny} any

before {permit | deny} any

after {permit | deny} any

no {permit | deny} any

Purpose

Allows or prevents access to all contexts (termination) and tunnels.

Command Mode

service access list

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **{permit | deny} any** command to allow or prevent access to all contexts and tunnels. The **permit any** command inserted at the end of a service access list has the effect of permitting anything that was not specifically denied. That way, nothing is denied by the implicit **deny any** that occurs at the end of every service access list.

Use the **before** form of this command to specify an existing statement in the access list before which you want to insert the next new statement that you create. All new statements will then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access list after which you want to insert the next new statement that you create. All new statements will then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example configures a service access list such that termination in a particular context is denied, and the **permit any** command is used to allow everything else:

```
[local]RedBack(config)#service access-list no_corps
[local]RedBack(config-service)#deny context corps
[local]RedBack(config-service)#permit any
```

Related Commands

{permit | deny} context
{permit | deny} domain
service access-list
show service access-list

{permit | deny} context

{**permit** | **deny**} **context** *ctx-name*

before {**permit** | **deny**} **context** *ctx-name*

after {**permit** | **deny**} **context** *ctx-name*

no {**permit** | **deny**} **context** *ctx-name*

Purpose

Allows or prevents access to the named context and all of its domains.

Command Mode

service access list

Syntax Description

ctx-name	Name of the context to be permitted or denied.

Default

None

Usage Guidelines

Use the **deny context** command to establish that the session cannot be terminated in the named context, nor can it be tunneled to any peer defined in that context. Conversely, the **permit context** command allows the session to be terminated in the named context, or tunneled to any peer defined in that context.

Use the **before** form of this command to specify an existing statement in the access list before which you want to insert the next new statement that you create. All new statements will then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access list after which you want to insert the next new statement that you create. All new statements will then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example denies termination in the context called `work`, permits termination in the context called `home`, and denies everything else (by virtue of the implicit **deny any** command at the end.)

```
[local]RedBack(config-service)#deny context work
[local]RedBack(config-service)#permit context home
```

Related Commands

{permit | deny} any
{permit | deny} domain
service access-list
show service access-list

{permit | deny} domain

{**permit** | **deny**} **domain** *dom-name*

before {**permit** | **deny**} **domain** *dom-name*

after {**permit** | **deny**} **domain** *dom-name*

no {**permit** | **deny**} **domain** *dom-name*

Purpose

Allows or prevents access to the named domain.

Command Mode

service access list

Syntax Description

dom-name	Name of the domain to be permitted or denied.

Default

None

Usage Guidelines

Use the {**permit** | **deny**} **domain** command to allow or prevent access to a specific domain. The domains (aliases) that this command can designate include context domains, Layer 2 Tunneling Protocol (L2TP) peer domains, L2TP group domains, and Layer 2 Forwarding (L2F) domains. This command is particularly useful in prohibiting access to a tunnel that would otherwise be available (due to a **domain** command in the same context as the one in which the tunnel is defined) for dynamic service selection.

Use the **before** form of this command to specify an existing statement in the access list before which you want to insert the next new statement that you create. All new statements will then follow one another in succession until you issue another positioning command.

Use the **after** form of this command to specify an existing statement in the access list after which you want to insert the next new statement that you create. All new statements will then follow one another in succession until you issue another positioning command.

Use the **no** form of this command to delete an individual statement in the access list. If you enter a statement that does not exist (or enter an existing statement incorrectly), an error message is displayed.

Examples

The following example shows using the **deny domain** command to disallow access to a particular tunnel. The **permit any** command allows access to everything else:

```
[local]RedBack(config-service)#deny domain redtunnel
[local]RedBack(config-service)#permit any
```

Related Commands

{permit | deny} any
{permit | deny} context
service access-list
show service access-list

service access-list

service access-list *list-name*

no service access-list *list-name*

Purpose

Creates or selects a service access list and enters service access list configuration mode.

Command Mode

global configuration

Syntax Description

list-name	Name of a new or existing service access list.

Default

None

Usage Guidelines

Use the **service access-list** command to create or select a service access list and enter service access list configuration mode where you can create the statements that make up the list or edit an existing list.

Service access lists restrict the services (contexts and domains) available to subscribers on a per-circuit basis. Service access lists are created in global configuration mode, and configured in service access list configuration mode. A list can then be applied in several ways: to a circuit in circuit configuration mode (**bind authentication** command), to a port in port configuration mode (**bind authentication** command), to a Layer 2 Tunneling Protocol (L2TP) peer in L2TP configuration mode (**session-auth** command), or to a Layer 2 Forwarding (L2F) peer in L2F configuration mode (**session-auth** command).

Use the **no** form of this command to delete the named service access list.

Examples

The following example creates a new service access list called `unsecure_only` and enters service access list configuration mode:

```
[local]RedBack(config)#service access-list unsecure_only
[local]RedBack(config-service)#
```

Related Commands

bind authentication
session-auth—L2F configuration mode
session-auth—L2TP configuration mode
show service access-list

show service access-list

show service access-list [*list-name* [**circuits**]]

Purpose

Displays the contents of a specific service access list or of all service access lists.

Command Mode

administrator exec

Syntax Description

list-name	Optional. Name of a specific service access list for which information is to be displayed.
circuits	Optional if you use the *list-name* argument. Specifies that the display is to include all the circuits or ports to which the named service access list has been applied.

Default

If no optional arguments or keywords are specified, information for all service access lists is included in the display. The display does not include the circuits or ports to which the service access lists have been applied.

Usage Guidelines

Use the **show service access-list** command to display one or all service access lists. The display is limited to a specific service access list if the optional *list-name* argument is included. If you specify a particular list, you can also specify that you want the display to include all circuits or ports to which that list has been applied.

Examples

The following example requests information about all service access lists and displays the results:

```
[local]RedBack#show service access-list

service access-list = level_1
   deny domain isp1
   deny context play
   permit any
```

```
service access-list = level_2
   deny domain corp1.com
   permit context home
```

The following example shows requesting information about a specific access list and the names of all the circuits or ports to which that list has been applied:

```
[local]RedBack#show service access-list level_2 circuits

service access-list = level_2
   deny domain corp1.com
   permit context home

   circuits applied:
      pppoe 00001
      b-1483 04.0.010.00010
```

The following example shows the same command, issued on a Subscriber Management System (SMS) 10000 device:

```
[local]RedBack#show service access-list level_2 circuits

service access-list = level_2
   deny domain corp1.com
   permit context home

   circuits applied:
      pppoe 00-00001
      b-1483 04.0.010.00010
```

Related Commands

bind authentication
service access-list
session-auth—L2F configuration mode
session-auth—L2TP configuration mode

Part 11

AAA and RADIUS

AAA Commands

This chapter describes the commands used to configure subscriber authentication, authorization, and accounting (AAA) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure AAA features, and configuration examples, see the "Configuring AAA" chapter in the *Access Operating System (AOS) Configuration Guide*.

aaa accounting

When used in context configuration mode, the command syntax is:

aaa accounting {**administrator** | **subscriber** | **tunnel**} {**none** | **radius**}

{**no** | **default**} **aaa accounting**

When used in global configuration mode, the command syntax is:

aaa accounting subscriber radius

{**no** | **default**} **aaa accounting subscriber radius**

Purpose

Enables the sending of Remote Authentication Dial-In User Service (RADIUS) messages for authentication, authorization, and accounting (AAA), either globally or per context.

Command Mode

context configuration
global configuration mode

Syntax Description

When used to enable RADIUS-based AAA on a per-context basis (in context configuration mode), the syntax description is:

administrator	Specifies that the setting is used for administrators.
subscriber	Specifies that the setting is used for subscribers.
tunnel	Specifies that the setting is used for tunnels.
none	Disables RADIUS-based accounting.
radius	Enables RADIUS-based accounting.

When used to enable RADIUS-based global AAA (in global configuration mode), the syntax description is:

subscriber	Specifies that the setting is used for subscribers.
radius	Enables RADIUS-based accounting.

Default

Global and context-specific RADIUS-based accounting are disabled.

Usage Guidelines

Use the **aaa accounting** command to enable the sending of RADIUS messages for AAA, either globally or per-context. At least one RADIUS server must be configured before any messages can be sent. The IP address and other parameters of the RADIUS servers are configured in the local context. To enable two-stage accounting, a RADIUS server must also be configured in a non-local context. In two-stage accounting, data for the context is sent to both the global RADIUS servers and the context-specific RADIUS servers.

When used in context configuration mode, this command can only enable sending of accounting packets that include packet and byte counts for a circuit if the **counters** command is configured in the ATM profile or Frame Relay profile referenced by the circuit to which the subscriber is bound.

Use the **no** or **default** form of this command, or specify the **none** keyword (when used in context configuration mode) to disable the sending of RADIUS accounting messages.

Examples

The following example configures the system to send RADIUS messages for `administrator` accounting for a specific context:

```
[local]RedBack(config-ctx)#aaa accounting administrator radius
```

Related Commands

counters—ATM configuration mode
counters—Frame Relay configuration mode
radius accounting server
radius server

aaa authentication administrator

aaa authentication administrator {**local** | **radius**}

Purpose

Determines whether administrators are authenticated by the Subscriber Management System (SMS) device local configuration or by a Remote Authentication Dial-In User Service (RADIUS) server.

Command Mode

context configuration

Syntax Description

local	Specifies that administrators are authenticated by the local configuration.
radius	Specifies that administrators are authenticated by a RADIUS server.

Default

Administrators are authenticated by the SMS device local configuration.

Usage Guidelines

Use the **aaa authentication administrator** command to specify whether administrators are to be authenticated by the SMS device local configuration or by a RADIUS server.

It is possible to enter the **aaa authentication administrator** command in sequence; once with the **radius** keyword and then again using the **local** keyword. In that case, authentication of administrators is first attempted by the RADIUS server. However, if the server is not reachable, or is not responding, the SMS device local database performs authentication.

Examples

The following example configures the SMS device to authenticate all administrators using the local configuration:

```
[local]RedBack(config-ctx)#aaa authentication administrator local
```

Related Commands

aaa accounting
radius server

aaa authentication re-try

aaa authentication re-try *minutes*

{**no** | **default**} **aaa authentication re-try**

Purpose

Configures the Subscriber Management System (SMS) device to periodically attempt to rebind unbound subscribers after authentication failure, or to attempt to connect Ethernet-encapsulated sessions after connection attempt failure.

Command Mode

context configuration

Syntax Description

minutes	Number of minutes the system waits before attempting to rebind or reconnect. The range is 1 through 1,000.

Default

Upon authentication failure, the SMS device does not attempt to rebind unbound subscribers. Upon failure to connect Ethernet-encapsulated sessions, the SMS device does not attempt connection any further.

Usage Guidelines

If authentication for a subscriber succeeds, the circuit to which the subscriber is bound is brought up and functions normally. By default, if authentication fails, the circuit remains unbound. Use the **aaa authentication re-try** command to direct the SMS device to try to rebind the subscriber to the circuit after the duration specified by the *minutes* argument.

Administrators who authenticate subscribers via a Remote Authentication Dial-In User Service (RADIUS) server generally use this feature. To provision a new subscriber, the administrator adds the appropriate entry into the RADIUS database, and sets up the subscriber's customer premise equipment (CPE).

This feature works only for subscribers bound to circuits using bridged RFC 1483 encapsulation or bridged RFC 1490 encapsulation. It does not work for subscribers using Point-to-Point Protocol (PPP) encapsulation.

You can also use this command in conjunction with Ethernet over Layer 2 Tunneling Protocol (L2TP). The connection of an Ethernet-encapsulated session is not attempted until data is received over the circuit or port. Once data is received, a connection attempt is made. The *minutes* argument in this command is the number of minutes after which the SMS device tries again to establish a session to the tunnel peer if the previous attempt failed. If the default setting of this command is used, no additional attempts to establish a session are made if the first attempt fails.

Use the **no** or **default** form of this command to reset the SMS device to its default behavior, where it does not attempt to rebind unbound subscribers, or make additional attempts to establish a session to a tunnel peer.

Example

The following example sets the period between rebind attempts to `90` minutes:

```
[local]RedBack(config-ctx)#aaa authentication re-try 90
```

Related Commands

aaa authentication subscriber
bind subscriber

aaa authentication subscriber

When used in context configuration mode, the command syntax is:

aaa authentication subscriber {**local** [**radius**] | **radius** [**local**] | **none**}

When used in global configuration mode, the command syntax is:

aaa authentication subscriber radius

Purpose

Sets subscribers to be authenticated either by the Subscriber Management System (SMS) device local configuration or by a Remote Authentication Dial-In User Service (RADIUS) server, on either a global or per context basis.

Command Mode

context configuration
global configuration

Syntax Description

When used on a per-context basis (in context configuration mode), the syntax description is:

local	Sets subscribers to be authenticated by the local configuration. If used as an optional keyword following the **radius** keyword, establishes that the local database is to be used for authentication in the event that the RADIUS server was not reachable.
radius	Sets subscribers to be authenticated by a remote RADIUS server. If used as an optional keyword following the **local** keyword, establishes that the RADIUS server is to be used for authentication in the event that no corresponding subscriber record was found in the local database.
none	Specifies that authentication of subscribers is not required—all access succeeds.

When used in global configuration mode, the syntax is:

radius	Sets subscribers to be authenticated by a remote RADIUS server.

Default

Subscribers are authenticated by the SMS device local configuration.

Usage Guidelines

Use the **aaa authentication subscriber** command to set subscribers to be authenticated either by the SMS device local configuration or by a RADIUS server, on either a global or per-context basis.

You can us the **local** and **radius** keywords together to specify that one method of authentication is to be attempted first, followed by the other. If you enter the **local** keyword, followed by the **radius** keyword, authentication is attempted first by the local configuration. If the subscriber record cannot be found locally, authentication is attempted by the RADIUS server. If you enter the **radius** keyword, followed by the **local** keyword, authentication is attempted by the local database in the event that the RADIUS server cannot be reached.

To disable authentication of subscribers in a context, use the **none** keyword. In that case, the Access Operating System (AOS) does not read any of the subscriber records configured in the current context, except for the default subscriber record. This means that IP addresses, routes, and Address Resolution Protocol (ARP) entries within individual subscriber records are not installed. The **none** keyword is typically used when many circuits are bound to identical subscriber information and user authentication is not required, such as when circuits are bound using the **bind auto-subscriber** command, and when Dynamic Host Configuration Protocol (DHCP) is used to obtain IP addresses for subscribers' hosts.

When used in global configuration mode, the **aaa authentication subscriber** command turns on global RADIUS authentication for the SMS device. The IP addresses and other parameters of the global RADIUS servers are configured in the local context.

The global configuration use of this command overrides the context configuration use. The result is that when global RADIUS authentication is enabled, configuration of context-specific RADIUS authentication servers is permitted, but ignored. You will see a warning to this effect if you try to configure a context-specific server when global RADIUS authentication is enabled.

Examples

The following example configures the system to authenticate all subscriber sessions in a specific context using the RADIUS protocol:

```
[local]RedBack(config-ctx)#aaa authentication subscriber radius
```

Related Commands

aaa accounting
bind auto-subscriber
radius server
subscriber

aaa authorization access-list

aaa authorization access-list radius

default aaa authorization access-list

Purpose

Specifies that an access control list can be downloaded from a Remote Authentication Dial-In User Service (RADIUS) server if the access control list is not found in the local configuration.

Command Mode

context configuration

Syntax Description

radius	Specifies that access control lists can be downloaded from the RADIUS server.

Default

Downloading of access control lists from a RADIUS server is disabled for the context.

Usage Guidelines

Use the **aaa authorization access-list** command to enable the downloading of an access control list from the RADIUS server in the event that a requested access control list does not exist in the local configuration. Once an access control list is downloaded from the RADIUS server, it remains available until no more bound subscribers reference it. At that time, the list is deleted from the system.

Use the **clear access-list** command (see Chapter 37, “IP Access Control List Commands”) to dereference one or all downloaded access control lists from bound subscribers. The **no ip access-list** command has no effect on downloaded access control lists.

Use the **default** form of this command to disable downloading of access control lists from the RADIUS server.

Note This command description also appears in Chapter 37, “IP Access Control List Commands.”

Examples

The following command configures the context `shore` so that the Access Operating System (AOS) looks for an access control list via RADIUS when there is no locally defined access list that matches the name specified:

```
[local]RedBack(config-config)#context shore
[local]RedBack(config-ctx)#aaa authorization access-list radius
```

Related Commands

clear access-list
show ip access-list

aaa authorization circuit

aaa authorization circuit radius

default aaa authorization circuit

Purpose

Specifies the means by which circuits are defined when using authentication, authorization, and accounting (AAA) circuit configuration.

Command Mode

context configuration

Syntax Description

radius	Specifies that circuits are to be defined via Remote Authentication Dial-In User Service (RADIUS).

Default

Circuit definition is done by RADIUS when AAA circuit configuration is being used.

Usage Guidelines

Use the **aaa authorization circuit** to specify the means by which circuits are defined when using AAA circuit configuration. At this time, RADIUS is the only AAA circuit definition option.

Use the **default** form of this command to set the circuit definition method to RADIUS.

Examples

The following example shows setting up AAA circuit configuration to be done via RADIUS:

```
[local]RedBack(config-ctx)#aaa authorization circuit radius
```

Related Commands

atm pvc explicit
atm pvc on-demand
frame-relay pvc explicit
frame-relay pvc on-demand

aaa authorization gre

aaa authorization gre {**local** | **radius**}

default aaa authorization gre

Purpose

Determines whether the generic routing encapsulation (GRE) peers are authorized by the local configuration or by a Remote Authentication Dial-In User Service (RADIUS) server.

Command Mode

context configuration

Syntax Description

local	Specifies that GRE tunnels are authorized through the local configuration.
radius	Specifies that GRE tunnels are authorized through a RADIUS server.

Default

GRE tunnels are authorized through the local configuration.

Usage Guidelines

Use the **aaa authorization gre** command to specify the means by which GRE peers are authorized. If you want to enable GRE circuit autoconfiguration (using the **gre-circuit** creation command), you must specify the **radius** keyword.

Use the **default** form of this command to specify that GRE tunnels are to be authorized by the local configuration.

Examples

The following example specifies that GRE tunnels are authorized through a RADIUS server:

```
[local]RedBack(config-ctx)#aaa authorization gre radius
```

Related Commands

gre-circuit creation

aaa authorization tunnel

aaa authorization tunnel {**local** | **radius**}

default aaa authorization tunnel

Purpose

Determines whether Layer 2 Tunneling Protocol (L2TP) peers are authorized by the Subscriber Management System (SMS) device local configuration or by a Remote Authentication Dial-In User Service (RADIUS) server.

Command Mode

context configuration

Syntax Description

local	Specifies that L2TP peers are authorized by the local configuration.
radius	Specifies that L2TP peers are authorized by a RADIUS server.

Default

L2TP peers are authorized by the SMS device local configuration.

Usage Guidelines

Use the **aaa authorization tunnel** command to specify whether L2TP peers are to be authorized by the SMS device local configuration or by a RADIUS server. Specify the **radius** keyword if you want to configure L2TP groups and peers using the **l2tp-group name** and **l2tp-peer name** commands, respectively, in context configuration mode. In addition, specify the **radius** keyword if you want to perform Dialed Number Identification Service (DNIS)-based tunnel switching via RADIUS. In this case, you must also use the **dnis** command in L2TP configuration mode.

Use the **default** form of this command to specify that L2TP peers are to be authorized by the local configuration.

Examples

The following command configures the system to use a remote RADIUS server when authorizing L2TP peers:

```
[local]RedBack(config-ctx)#aaa authorization tunnel radius
```

Related Commands

aaa accounting
dnis
l2tp attribute calling-number real-circuit-id
l2tp-peer name
radius server

aaa binding

aaa binding explicit-only

default aaa binding

Purpose

Configures a context to be ineligible for dynamic binding by a Point-to-Point Protocol (PPP) session.

Command Mode

context configuration

Syntax Description

explicit-only	Specifies that dynamic binding by a PPP session is not allowed in the context or its domains.

Default

Dynamic binding is allowed.

Usage Guidelines

Use the **aaa binding** command to affect how PPP sessions are permitted to bind to the context in which the command is entered. When the **aaa binding explicit-only** command is used, the context and its domains become ineligible for dynamic binding by a PPP session. Sessions can then only bind to the context if:

- The session arrives over a circuit, tunnel, or port to which a service access list has been applied that permits that context or domain (using the **bind authentication** ... **service-group** *group-name* command or the **session-auth** ... **service-group** *group-name* command, in the case of tunnels).
- The context is explicitly named in a **bind authentication** ... **context** *ctx-name* command (or **session-auth** ... **context** *ctx-name* command, in the case of tunnels).

If the **aaa binding** command is not used, dynamic binding is allowed in the context and its domains. Use the **default** form of this command to return to allowing dynamic binding in the context and its domains.

Examples

The following example configures a context to be ineligible for dynamic binding by a PPP session:

```
[local]RedBack(config)#context precision
[local]RedBack(config-ctx)#aaa binding explicit-only
```

Based on this example, the following behaviors result:

- A permanent virtual circuit (PVC) with the **bind authentication** {**pap** | **chap** | **chap pap**} command configured (no context or service-group name specified) would experience a change in behavior when the **aaa binding explicit-only** command is used. Sessions are not allowed to bind to any contexts (or tunnels in those contexts) where the **aaa binding explicit-only** command is used. The same would be true for a tunnel with the **session-auth** {**pap** | **chap** | **chap pap**} command configured (no context or service-group name specified).
- A PVC with the **bind authentication** {**pap** | **chap** | **chap pap**} **context** *ctx-name* command configured, with the `precision` context specified, would experience no change in behavior, because sessions are already explicitly restricted to the `precision` context. The **aaa binding explicit-only** command imposes no additional restriction. The same would be true for a tunnel with the **session-auth** {**pap** | **chap** | **chap pap**} **context** *ctx-name* command configured, with the `precision` context specified.
- A PVC with the **bind authentication** {**pap** | **chap** | **chap pap**} **service-group** *group-name* command configured would experience no change in behavior, because whether or not sessions are allowed to terminate in a context is based on the criteria specified by the service access list. The **aaa binding explicit-only** command imposes no additional restriction. The same would be true for a tunnel with the **session-auth** {**pap** | **chap** | **chap pap**} **service-group** *group-name* command configured.
- A PVC with the **bind session** *peer-name ctx-name* command configured, with the `precision` context specified, would experience no change in behavior. All sessions would proceed through the tunnel, regardless of the **aaa binding explicit-only** command for the `precision` context.

Related Commands

bind authentication
bind session
debug aaa
session-auth

aaa default-domain

aaa default-domain *dom-name* [**username-format** {**domain** | **username**} *separator-char*]

{**no** | **default**} **aaa default-domain** *dom-name*

Purpose

Defines a default domain to be used for authentication when a domain name is not provided, that is, when the username is unstructured.

Command Mode

global configuration

Syntax Description

dom-name	String to be concatenated to the provided username.
username-format	Keyword preceding the specification of the portion of the structured username that is to go first.
domain	Specifies that the *domain* portion of the structured username is to precede the *user* portion.
username	Specifies that the *user* portion of the structured username is to precede the *domain* portion.
separator-char	Character that separates the *user* portion from the *domain* portion of the structured username. The possible values are %, -, @, \\, #, and /. When you want the separator character to be a backslash (\), you must enter it on the command line as two backslashes (\\). A single backslash has a reserved meaning in the Access Operating System (AOS).

Default

If this command is not used, no default domain is appended to unstructured usernames before submission to authentication, authorization, and accounting (AAA) for authentication. If the command is used without the optional construct, the specified *domain-name* is appended in the AOS default format of *@domain*. The optional construct can dictate a different format.

Usage Guidelines

Use the **aaa default-domain** command to define a default domain to be used for authentication when a domain name is not provided, that is, when the username is unstructured.

This command works in conjunction with the **aaa username-format** command. The **aaa username-format** command defines the allowable formats for structured usernames. The **aaa default-domain** command specifies how a username, that is not formatted according to any of these allowable formats (an unstructured username), is to be handled.

Before sending a username to AAA for authentication, AOS first compares it to each allowable username format in turn, looking for a format match. If no match is found, the name is then treated as an unstructured username according to the behavior established by the **aaa default-domain** command.

If the optional construct is not used in the **aaa default-domain** command, the specified domain-name is appended to the unstructured username in the AOS default format of *@domain*, and the result is submitted for authentication. The optional construct is used to dictate a different structure. Specifically, it specifies whether the *domain* portion or the *user* portion of the username should go first, and it specifies which of the valid characters is to be used as a separator between the two portions.

This command does not affect the console, which only allows operators or administrators to authenticate in the local context.

Use the **no** or **default** form of this command to disable the feature so that no default domain is appended to the username before being submitted for authentication.

Examples

Consider the following series of configuration commands:

```
[local]RedBack(config)#aaa username-format username @
[local]RedBack(config)#aaa username-format domain %
[local]RedBack(config)#aaa default-domain allnation username #
```

Based on this configuration, the following usernames would be submitted to AAA for authentication as indicated in Table 40-1:

Table 40-1 Username Treatment with a Default Domain

Username as Provided	Username as Submitted for Authentication	Notes
mary	mary#allnation	Default-domain takes effect because the name as submitted does not match any allowable format.
mary@local	mary@local	Submitted unchanged because the name matches the first configured username format.
mary/local	mary/local#allnation	Default-domain takes effect and treats the entire submitted name as the user portion of a structured username.
caliope%mary	caliope%mary	Submitted unchanged because the name matches the second configured username format.

Suppose now that the **aaa default-domain** command is not entered:

```
[local]RedBack(config)#aaa username-format username @
[local]RedBack(config)#aaa username-format domain %
```

The same usernames would be treated as shown in Table 40-2:

Table 40-2 Username Treatment Without a Default Domain

Username as Provided	Username as Submitted for Authentication	Notes
mary	mary	No default-domain has been specified, so nothing is appended to the submitted *user* portion of the name.
mary@local	mary@local	Submitted unchanged because the name as submitted matches the first configured username format.
mary/local	mary/local	No default-domain has been specified, so nothing is appended to the submitted *user* portion of the name.
caliope%mary	caliope%mary	Submitted unchanged because the name as submitted matches the second configured username format.

The following example uses the **aaa default-domain** command, but no username formats are specified:

```
[local]RedBack(config)#aaa default-domain allnation username #
```

The same usernames in the previous example would be treated as shown in Table 40-3:

Table 40-3 Username Treatment Without Specified Formats

Username as Provided	Username as Submitted for Authentication	Notes
mary	mary#allnation	No username formats were configured, which means that the AOS default of *user@domain* is in effect. The *domain* comes from the **aaa default-domain** command.
mary@local	mary@local	Submitted unchanged because the name as submitted matches the AOS default format for structured usernames.
mary/local	mary/local#allnation	Default-domain takes effect and treats the entire submitted name as the user portion of a structured username.
caliope%mary	caliope%mary#allnation	Default-domain takes effect and treats the entire submitted name as the user portion of a structured username.

Related Commands

aaa username-format
context
domain
radius strip-domain

aaa delay-start-record

aaa delay-start-record

{**no** | **default**} **aaa delay-start-record**

Purpose

Delays sending of the accounting start record to the Remote Authentication Dial-In User Service (RADIUS) server until after the Internet Protocol Control Protocol (IPCP) comes up, so that an IP address can be included in the record. Only relevant for Point-to-Point Protocol (PPP) sessions.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

The accounting start record is sent before IPCP comes up and does not contain an IP address.

Usage Guidelines

The RADIUS accounting start record is normally sent to the RADIUS server before IPCP comes up. This prevents including an IP address with the accounting start record because it is not yet known. Use the **aaa delay-start-record** command when you want to hold off on sending the accounting start record for PPP sessions until after IPCP comes up so that an IP address can be included. The IP address is sent to RADIUS in the Framed-IP-Address attribute.

Use the **no** or **default** form of this command to disable delay of the accounting start record.

Examples

The following example delays sending the accounting start record:

```
[local]RedBack(config-ctx)#aaa delay-start-record
```

Related Commands

aaa update

aaa hint ip-address

aaa hint ip-address

no aaa hint ip-address

Purpose

Causes the Subscriber Management System (SMS) device to send an unused IP address out of its local pool to the Remote Authentication Dial-In User Service (RADIUS) server in the Framed-IP-Address attribute of the RADIUS authentication request.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

The AAA hint feature is disabled, that is, no IP address is sent to the RADIUS server in the Framed-IP-Address attribute of the RADIUS authentication request.

Usage Guidelines

Use the **aaa hint ip-address** command to direct the SMS device to send an unused IP address out of its local pool to the RADIUS server in the Framed-IP-Address attribute of the RADIUS authentication request.

The IP address selected from the local IP pool is intended as a hint to the RADIUS server that the selected address is preferred. The RADIUS server may choose to honor the hint or override it with a different IP address. The SMS device only uses the address if the RADIUS server confirms that it is acceptable. The SMS device responds to the RADIUS response according to the decision tree outlined in the "Configuring AAA" chapter of the *Access Operating System (AOS) Configuration Guide*.

Use the **no** form of this command to disable the AAA hint feature.

Examples

The following example enables the AAA hint feature in the `customers` context:

```
[local]Redback(config)#context customers
[local]Redback(config-cxt)#aaa hint ip-address
```

Related Commands

debug aaa

aaa last-resort

aaa last-resort context *ctx-name*

no aaa last-resort

Purpose

Specifies the context in which authentication of a username should be attempted if the username does not contain a domain or context that has been configured in the system.

Command Mode

global configuration

Syntax Description

context *ctx-name*	Name of the last resort context.

Default

No last resort context is configured.

Usage Guidelines

Use the **aaa last-resort** command to establish a context in which authentication of a username is to be attempted whenever the domain portion of the username provided can not be matched to any configured context or domain.

At the time you enter this command, the Access Operating System (AOS) does not check to ensure you specify a valid context. When a user attempts to connect, and AOS attempts to validate the user in the last resort context, an error message is displayed if the context does not exist.

Only one last resort context can be in effect at a time. If you want to change the last resort context, create a new one and it overwrites the existing one.

If you are using global Remote Authentication Dial-In User Service (RADIUS), this command has no effect, because the RADIUS server is responsible for authenticating users, and specifying the appropriate context for each authenticated user.

Use the **no** form of this command to remove the last resort context.

Examples

Suppose the configuration includes three contexts, `california`, `nevada` and `otherstates`. A username `jill@arizona` is submitted for authentication, but there is no configured context called `arizona`. The following example shows configuring the system in such a way that `jill@arizona` would be submitted for authentication in the context `otherstates`:

```
[local]RedBack(config)#aaa last-resort context otherstates
```

Related Commands

aaa default-domain
aaa username-format

aaa max-subscribers

aaa max-subscribers *sub-num*

default aaa max-subscribers

Purpose

Limits the number of subscribers that can be simultaneously bound to a context.

Command Mode

context configuration

Syntax Description

sub-num	Maximum number of subscribers that can be simultaneously bound to the context. Must be equal to or less than the hard limit imposed by the platform. The hard limit for each SMS device is: • SMS 500—2,000 • SMS 1000 or SMS 1800 with FE1 module—4,000 • SMS 1000 or SMS 1800 with FE2 module (48 MB RAM)—8,000 • SMS 10000—100,000

Default

There is no limit (other than the hard limit imposed by the platform) to the number of subscribers within a context.

Usage Guidelines

Use the **aaa max-subscribers** command to limit the number of subscribers that can be simultaneously bound to a context. This command is typically used to impose an administrative restriction on the maximum number of subscribers terminating in a context in environments where dynamic binding is used.

By default, there is no limit to the number of subscribers that can be bound to a context, other than the hard limits imposed by the platform. Use the **default** form of this command to restore that default.

Examples

The following example sets the maximum number of subscribers for the local context to 100. The 25 bridged RFC 1483 circuits using the **bind auto-subscriber** command take up a quarter of that allocation leaving room for only 75 Point-to-Point (PPP) sessions that can be simultaneously terminated in the local context.

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#aaa max-subscribers 100
[local]RedBack(config)#port atm 2/0
[local]RedBack(config-port)#atm pvc 0 1 through 25 pro ubr encaps bridge1483
[local]RedBack(config-pvc)#bind auto-subscriber joe local
[local]RedBack(config-pvc)#exit
[local]RedBack(config-port)#atm pvc 0 26 through 2047 pro ubr encaps ppp
[local]RedBack(config-pvc)#bind authentication pap
```

The following example restores the factory default of no limit:

```
[local]RedBack(config-ctx)#default aaa max-subscribers
```

Related Commands

bind authentication
bind auto-subscriber
bind subscriber

aaa min-subscribers

aaa min-subscribers *sub-num*

{**no** | **default**} **aaa min-subscribers**

Purpose

Guarantees a minimum number of subscriber slots reserved for a context.

Command Mode

context configuration

Syntax Description

sub-num	Minimum number of subscriber slots reserved for the context.

Default

There is no reserved minimum.

Usage Guidelines

Use the **aaa min-subscribers** command to ensure that a certain number of the total number of subscribers possible on the system are reserved for a particular context. Combined, all the guaranteed minimums for all the contexts must not exceed the hard limit imposed by the platform.

You can also reserve a minimum number of subscriber slots on the tunnel peer level. The total number of subscribers reserved on the tunnel peer level cannot exceed the number reserved for the context as a whole. See the description of the **l2x profile** command in either Chapter 25, “L2TP Commands,” or Chapter 26, “L2F Commands” for more information on reserving subscriber slots for tunnel peers.

By default, there is no reserved minimum number of subscriber slots in a context. Use either the **no** or **default** form of this command to return to that default.

Examples

The following example sets the reserved minimum number of subscriber slots for the context `trinity` to `1000`:

```
[local]RedBack(config)#context trinity
[local]RedBack(config-ctx)#aaa min-subscribers 1000
```

Related Commands

bind subscriber
l2x profile—L2F configuration mode
l2x profile—L2TP configuration mode
profile—L2F configuration mode
profile—L2TP configuration mode
show subscribers

aaa terse-messages

aaa terse-messages

{**no** | **default**} **aaa terse-messages**

Purpose

Disables the use of more descriptive authentication failure messages.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

More descriptive authentication-failure messages are printed by default.

Usage Guidelines

Use the **aaa terse-messages** command to prevent more descriptive authentication-failure messages from being presented to the user. When this command is enabled, the Access Operating System (AOS) displays `Authentication Failure` for all authentication failure reasons. When disabled, AOS attempts to be more verbose, such as reminding the user when a username is not in a configured structured-username format.

Use the **no** or **default** form of the command to see more descriptive authentication-failure messages.

Examples

The following example enables terse authentication failure messages:

```
[local]RedBack(config)#aaa terse-messages
```

The following example disables terse authentication failure messages:

```
[local]RedBack(config)#no aaa terse-messages
```

Related Commands

aaa authentication subscriber
aaa default-domain

aaa update

aaa update {*accounting-period* | **ipcp-up** | **dhcp-event**}

{**no** | **default**} **aaa update** {*accounting-period* | **ipcp-up** | **dhcp-event**}

Purpose

Enables periodic updates for subscriber accounts.

Command Mode

context configuration
global configuration

Syntax Description

accounting-period	Period (in minutes) between accounting updates. The range of values is 10 to 10,080.
ipcp-up	Specifies that a single update is to be sent right after the Internet Protocol Control Protocol (IPCP) comes up, but none after that.
dhcp-event	Specifies that the Access Operating System (AOS) is to generate an accounting packet for the Remote Authentication Dial-In User Service (RADIUS) server whenever an address is assigned.

Default

Updates for subscriber accounts are not performed.

Usage Guidelines

Use the **aaa update** command to have updated accounting records sent for each subscriber for the life of the subscriber's session. This command only has an effect when an accounting method is configured.

If you specify a value for the *accounting-period* argument, the first update is sent when IPCP first comes up. The time between subsequent updates is dictated by the *accounting-period* argument.

Use the **dhcp-event** keyword to enable the generation of an accounting packet for RADIUS every time an address is assigned, regardless of whether the Subscriber Management System (SMS) device is configured as a Dynamic Host Configuration Protocol (DHCP) server or as a DHCP relay. If the SMS device is configured as a DHCP server, it also generates a packet for RADIUS when a lease expires or is released. No packet is sent when a lease is renewed.

This command can be used in either global or context configuration mode. The global configuration takes precedence over the context configuration.

Almost all Remote Authentication Dial-In User Service (RADIUS) attributes that can be sent in an Accounting-Request packet may be present in an Accounting-Update record. See the "RADIUS Attributes" appendix in the *Access Operating System (AOS) Configuration Guide* for information about the RADIUS attributes that can be sent in an Accounting-Request packet.

Use the **no** or **default** form of this command to disable subscriber account updating.

Examples

The following example configures an update to be sent as soon as IPCP comes up, and every `20` minutes thereafter, for as long as the subscriber session lasts:

```
[local]RedBack(config-ctx)#aaa update 20
```

The following example configures a single update to be sent as soon as IPCP comes up, but no updates after that:

```
[local]RedBack(config-ctx)#aaa update ipcp-up
```

The following example enables generation of accounting packets for RADIUS in response to DHCP events:

```
[local]Redback(config)#aaa update dhcp-event
```

Related Commands

aaa accounting
radius server

aaa username-format

aaa username-format {**domain** | **username**} *separator*

no aaa username-format {**domain** | **username**} *separator*

Purpose

Defines one or more schemas for matching the format of structured usernames.

Command Mode

global configuration

Syntax Description

domain	Specifies that the *domain* portion of the structured username is to precede the *user* portion.
username	Specifies that the *user* portion of the structured username is to precede the *domain* portion.
separator	Character that separates the *user* portion of the structured username from the *domain* portion. The possible values are %, -, @, \\, #, and /. When you want the separator character to be a backslash (\), you must enter it here as two backslashes (\\). A single backslash has a reserved meaning in the Access Operating System (AOS).

Default

If no username formats are specified with this command, the Access Operating System (AOS) default format of *username@domain* is checked for a format match.

Usage Guidelines

Use the **aaa username-format** command to define one or more schemas for matching the format of structured usernames.

This command can be used multiple times to create a list of formats against which an incoming username is matched. The first format configured is checked first for a match, then the second, and so on until a match is found or the configured username formats are exhausted. If no match is found, the username is considered to be unstructured, and is treated according to the behavior defined by the **aaa default-domain** command.

If no username formats are explicitly defined with the **aaa username-format** command, the AOS default format of *username@domain* is checked for a match. This default is not checked for a match if other formats are configured unless it, too, is specifically configured. In other words, the format *username@domain* is not automatically checked for a match, unless no other structured username formats are configured.

Use the **no** form of this command to remove the specified format from those considered to be valid structured-username formats.

Examples

The following example shows configuring two structured-username formats:

```
[local]RedBack(config)#aaa username-format username @
[local]RedBack(config)#aaa username-format domain %
```

Related Commands

aaa default-domain
show username-format

debug aaa

debug aaa {**authentication** | **authorization** | **accounting** | **ip-pool**}

no debug aaa {**authentication** | **authorization** | **accounting** | **ip-pool**}

Purpose

Enables the logging of debugging messages for authentication, authorization, and accounting (AAA).

Command Mode

administrator exec

Syntax Description

authentication	Enables authentication debugging.
authorization	Enables authorization debugging.
accounting	Enables accounting debugging.
ip-pool	Enables IP pool debugging.

Default

AAA debugging is disabled.

Usage Guidelines

Use the **debug aaa** command to enable AAA debugging. When debugging is enabled, all messages are logged. Use the **logging console** or **terminal monitor** commands to display the messages in real time.

The output of the **debug aaa ip-pool** command is a subset of the output of the **debug aaa authorization** command. Use the **ip-pool** keyword when you want IP pool debugging, but do not want all the non-IP debug messages that the **debug aaa authorization** command generates.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable AAA debugging.

Examples

The following example enables authentication debugging:

```
[local]RedBack#debug aaa authentication
[local]RedBack#show debugging

AAA:
   Authentication debugging is on
```

The following example enables IP pool debugging:

```
[local]RedBack#debug aaa ip-pool
[local]RedBack#show debugging

AAA:
   Ip-pool debugging is on
```

The following example shows sample debugging messages when IP pool debugging is enabled:

```
01:37:29 1Feb2001: %AAA-7-YES_POOL:Got pool address 10.1.1.2 for user
“dan@local”.

01:45:51 1Feb2001:%AAA-7-POOL3:ipcp_lowerdown() returning IP-Pool
address.

01:45:51 1Feb2001:%AAA-7-POOL_DONE:Returning IP-Pool address 10.1.1.2 to
pool.
```

The following example shows a sample debugging message when authentication debugging is enabled, and there is an explicit binding violation (see the description of the **aaa binding explicit-only** command):

```
01:37:29 1Feb2001: Access denied. Context swbit need explicit binding.
```

Related Commands

debug ppp
logging console
show debugging
show log
terminal monitor

show username-format

show username-format

Purpose

Displays the current list of username formats defined in this Subscriber Management System (SMS) device.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show username-format** command to display all the currently configured username formats that can be submitted without modification to authentication, authorization, and accounting (AAA) for authentication. These formats are configured with the **aaa username-format** command in global configuration mode. If a username does not fit any of these formats, the name is considered to be an unstructured username and is treated according to the behavior defined in the **aaa default-domain** command, also in global configuration mode.

Examples

The following example shows requesting a list of configured formats for structured usernames and the resulting display:

```
[local]RedBack>show username-format

username@domain
domain%username
```

Related Commands

aaa default-domain
aaa username-format
radius strip-domain

RADIUS Commands

This chapter describes the commands used to configure the Access Operating System (AOS) to function as a Remote Authentication Dial-In User Service (RADIUS) client, enabling remote configuration of subscriber records.

For overview information, a description of the tasks used to configure RADIUS features, and configuration examples, see the "Configuring RADIUS" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug radius

debug radius {**accounting** | **attributes** | **authentication** | **authorization** | **packet**}

no debug radius {**accounting** | **attributes** | **authentication** | **authorization** | **packet**}

Purpose

Enables the logging of Remote Authentication Dial-In User Service (RADIUS) debugging messages.

Command Mode

administrator exec

Syntax Description

accounting	Enables RADIUS accounting debugging.
attributes	Enables RADIUS attribute debugging.
authentication	Enables RADIUS authentication debugging.
authorization	Enables RADIUS authorization debugging.
packet	Enables RADIUS packet-level debugging.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug radius** command to enable the logging of RADIUS debugging messages.

As a default, the debug output is sent to the log. If you want to have debug output sent to the console, you must enter the **logging console** global configuration command. If you are connected via Telnet, use the **terminal monitor** operator exec command.

Caution Debugging can severely affect system performance. Exercise caution when enabling debugging on a production system.

Use the **no** form of this command to disable the logging of RADIUS debugging messages.

Examples

The following example enables packet-level debugging for RADIUS:

```
[local]RedBack#debug radius packet
```

The following example enables debugging for RADIUS authentication:

```
[local]RedBack#debug radius authentication
```

The following example disables debugging for RADIUS authentication:

```
[local]RedBack#no debug radius authentication
```

Related Commands

logging console
radius server
radius timeout
radius max-retries
radius strip-domain
show debugging
terminal monitor

radius accounting algorithm

radius accounting algorithm {**first** | **round-robin**}

no radius accounting algorithm

Purpose

Specifies a load-balancing algorithm to use among multiple Remote Authentication Dial-In User Service (RADIUS) accounting servers.

Command Mode

context configuration

Syntax Description

first	Specifies that the first configured RADIUS server is always queried first.
round-robin	Specifies that RADIUS servers are queried in round-robin fashion.

Default

The Subscriber Management System (SMS) device uses the first configured RADIUS server first.

Usage Guidelines

Use the **radius accounting algorithm** command to specify a load-balancing algorithm to be used among multiple RADIUS accounting servers. When specified in the local context, the load-balancing algorithm that is selected is used globally by the SMS device.

You must configure RADIUS servers using the **radius accounting server** or **radius server** command prior to specifying an algorithm.

Use the **default** form of this command to reset the load-balancing algorithm to use the first configured RADIUS server first.

Example

The following example sets the load-balancing algorithm to `round-robin`:

```
[local]RedBack(config-ctx)#radius accounting algorithm round-robin
```

Related Commands

radius accounting deadtime
radius accounting max-outstanding
radius accounting max-retries
radius accounting server
radius accounting timeout
radius server

radius accounting deadtime

radius accounting deadtime *minutes*

default radius accounting deadtime

Purpose

Specifies the interval after which the Subscriber Management System (SMS) device is to treat a non-responsive Remote Authentication Dial-In User Service (RADIUS) accounting server as dead, and try to reach the server.

Command Mode

context configuration

Syntax Description

minutes	Deadtime interval in minutes. The range of values is 0 to 65,535; the default value is 5. The 0 value disables the feature.

Default

The SMS device waits five minutes before trying to reach a non-responsive RADIUS server.

Usage Guidelines

Use the **radius accounting deadtime** command to specify the interval after which the SMS device is to treat a non-responsive RADIUS accounting server as dead, and try to reach the server.

Use the **default** form of this command to reset the deadtime value to five minutes.

Examples

The following example sets the deadtime to `10` minutes:

```
[local]RedBack(config-ctx)#radius accounting deadtime 10
```

Related Commands

radius accounting algorithm
radius accounting max-outstanding
radius accounting max-retries
radius accounting server
radius accounting timeout

radius accounting max-outstanding

radius accounting max-outstanding *requests*

{**no** | **default**} **radius accounting max-outstanding**

Purpose

Configures the number of simultaneous outstanding accounting requests that can be sent by the Subscriber Management System (SMS) device to Remote Authentication Dial-In User Service (RADIUS) accounting servers.

Command Mode

context configuration

Syntax Description

requests	The number of simultaneous outstanding requests. The range of values is 1 to 256.

Default

The number of simultaneous outstanding accounting requests sent by the SMS device is 256.

Usage Guidelines

Use the **radius accounting max-outstanding** command if the RADIUS servers cannot handle the default of 256 simultaneous outstanding accounting requests that the SMS device can send to RADIUS accounting servers configured within the context.

Use the **no** or **default** form of this command to reset the maximum number of allowable outstanding requests to 256.

Examples

The following example limits the number of simultaneous outstanding requests to `128`:

```
[local]RedBack(config-ctx)#radius accounting max-outstanding 128
```

Related Commands

radius accounting algorithm
radius accounting deadtime
radius accounting max-retries
radius accounting server
radius accounting timeout

radius accounting max-retries

radius accounting max-retries *retries*

default radius accounting max-retries

Purpose

Configures the number of retransmissions by the Subscriber Management System (SMS) device if a Remote Authentication Dial-In User Service (RADIUS) does not send an acknowledgment.

Command Mode

context configuration

Syntax Description

retries	Number of times the SMS device is to retransmit a RADIUS accounting packet. The range of values is 1 to 2,147,483,647; the default value is 3.

Default

The SMS device sends three retransmissions.

Usage Guidelines

Use the **radius accounting max-retries** command to modify the retransmission behavior of the SMS device in the event that an acknowledgment is not received from a RADIUS accounting server within the configured interval.

If an acknowledgment is not received, each successive, configured server is tried (wrapping from the last server to the first, if necessary) until the maximum number of retransmissions is reached.

Use the **default** form of this command to reset the number of retries to three.

Example

The following example sets the retransmit value to 5:

```
[local]RedBack(config-ctx)#radius accounting max-retries 5
```

The following example resets the retransmit value to the default of 3:

```
[local]RedBack(config-ctx)#default radius accounting max-retries
```

Related Commands

radius accounting algorithm
radius accounting deadtime
radius accounting max-outstanding
radius accounting server
radius accounting timeout

radius accounting server

radius accounting server {*ip-address* | *hostname*} **key** *key* [**oldports** | **port** *udp-port*] [**max** *requests*]

no radius accounting server

Purpose

Configures Remote Authentication Dial-In User Service (RADIUS) accounting servers.

Command Mode

context configuration

Syntax Description

ip-address	IP address of the RADIUS accounting server.
hostname	Hostname of the RADIUS accounting server. Domain Name System (DNS) must be enabled to use the *hostname* argument. See the "Usage Guidelines" section of this command description.
key *key*	Authentication key used when communicating with the accounting server.
oldports	Optional. Designates the old RADIUS User Datagram Protocol (UDP) ports 1,645 and 1,646.
port *udp-port*	Optional. RADIUS accounting UDP port. The range of values is 1 to 65,536; the default value is 1,813.
max *requests*	Optional. Maximum number of outstanding accounting requests that can be sent to this server. The range of values is 1 to 256; the default value is 256. This value overrides the value set with the **radius accounting max-outstanding** command.

Default

Accounting data is sent to the same RADIUS servers to which the authorization requests are sent. UDP port 1,813 is the default UDP port.

Usage Guidelines

Use the **radius accounting server** command to configure a separate RADIUS accounting server as opposed to using the **radius server** command to configure one server to perform both authentication and accounting functions.

If you configure a RADIUS server or RADIUS accounting server in the local context, these servers perform authentication and accounting for the entire device. The Access Operating System (AOS) provides warnings if a context-specific authentication server is configured when global authentication is enabled.

To enable two-stage accounting, you must first configure a RADIUS server in a non-local context. In two-stage accounting, data for the context is sent to both the global RADIUS servers and the context-specific RADIUS servers.

Using the **port** keyword, you can configure multiple RADIUS servers on the same host by specifying a different UDP port for each server.

You can only use the *hostname* argument if DNS has been enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode. See Chapter 28, "DNS Commands" for descriptions of these commands.

Use the **no** form of this command to delete a previously configured RADIUS accounting server.

Examples

The following example defines a remote RADIUS accounting server with an IP address of `10.2.3.4`, the key `TopSecret,` and the default UDP port of 1813:

```
[local]RedBack(config-ctx)#radius accounting server 10.2.3.4 key TopSecret
```

The following example defines a remote RADIUS accounting server with the IP address `10.3.3.3`, the key `NotTooObvious`, and UDP port `4445`:

```
[local]RedBack(config-ctx)#radius accounting server 10.3.3.3 key NotObvious port 4445
```

Related Commands

aaa accounting
ip domain-lookup
ip domain-name
ip name-servers
radius accounting algorithm
radius accounting deadtime
radius accounting max-outstanding
radius accounting max-retries
radius accounting timeout
radius server

radius accounting timeout

radius accounting timeout *seconds*

default radius accounting timeout

Purpose

Sets the maximum time the Subscriber Management System (SMS) device is to wait for a response from a Remote Authentication Dial-In User Service (RADIUS) accounting server before assuming that a packet is lost.

Command Mode

context configuration

Syntax Description

seconds	Timeout period in seconds. The range of values is to 2,147,483,647; the default value is 10 seconds.

Default

The maximum time is 10 seconds.

Usage Guidelines

Use the **radius accounting timeout** command to set the maximum time the SMS device is to wait for a response from a RADIUS accounting server before assuming that a packet is lost.

Use the **default** form of this command to return to the default value of 10 seconds.

Examples

The following example sets the RADIUS accounting timeout to `30` seconds:

```
[local]RedBack(config-ctx)#radius accounting timeout 30
```

Related Commands

aaa accounting
radius accounting deadtime
radius accounting max-outstanding

radius accounting max-retries
radius accounting server
radius accounting timeout

radius algorithm

radius algorithm {**first** | **round-robin**}

default radius algorithm

Purpose

Specifies a load-balancing algorithm to use among multiple Remote Authentication Dial-In User Service (RADIUS) servers.

Command Mode

context configuration

Syntax Description

first	Specifies that the first configured RADIUS server is always queried first.
round-robin	Specifies that the RADIUS servers are queried in round-robin fashion.

Default

The Subscriber Management System (SMS) device queries the first configured server first.

Usage Guidelines

Use the **radius algorithm** command to specify a load-balancing algorithm to use among multiple RADIUS servers. When specified in the local context, the load-balancing algorithm that is selected is used globally by the SMS device.

You must configure RADIUS servers using the **radius server** command prior to specifying an algorithm.

Use the **default** form of this command to reset the SMS device to query the first configured server first.

Examples

The following example sets the algorithm to `round-robin`:

```
[local]RedBack(config-ctx)#radius algorithm round-robin
```

Related Commands

radius deadtime
radius max-outstanding
radius max-retries

radius server
radius strip-domain
radius timeout

radius attribute acct-session-id

radius attribute acct-session-id access-request

no radius attribute acct-session-id

Purpose

Enables the Subscriber Management System (SMS) device to send the Acct-Session-Id attribute in Access-Request packets for the current context in addition to sending it in Accounting-Request packets.

Command Mode

context configuration

Syntax Description

access-request	Specifies that the attribute is to be sent in Access-Request packets for the current context.

Default

The Acct-Session-Id attribute is only sent in Accounting-Request packets.

Usage Guidelines

Use the **radius attribute acct-session-id** command to configure the SMS device to send the Acct-Session-Id attribute in all Access-Request packets in addition to the default behavior of sending the attribute in Accounting-Request packets. When this command is enabled, the SMS device creates the Acct-Session-Id when it starts authentication, and then uses it in the Access-Request and Accounting-Request packets.

Use the **no** form of this command to disable the sending of the Acct-Session-Id attribute in Access-Request packets.

Examples

The following example configures the SMS device to send the Acct-Session-Id attribute in Access-Request packets:

```
[local]RedBack(config-ctx)#radius attribute acct-session-id access-request
```

Related Commands

debug radius
radius attribute calling-station-id
radius attribute connect-info
radius attribute filter-id
radius attribute medium-type
radius attribute nas-ip-address
radius attribute non-rfc-242
radius attribute tunnel password

radius attribute calling-station-id

radius attribute calling-station-id separator *character*

no radius attribute calling-station-id

Purpose

Configures the Subscriber Management System (SMS) device to send the Calling-Station-Id attribute in all Authentication and Accounting packets for the context.

Command Mode

context configuration

Syntax Description

separator *character*	Character that separates the elements of the attribute string.

Default

The Calling-Station-Id attribute is not sent.

Usage Guidelines

Use the **radius attribute calling-station-id** command to configure the SMS device to send the Calling-Station-Id attribute in all Authentication and Accounting packets for the context.

When this command is in effect, the SMS device sends the Remote Authentication Dial-In Service (RADIUS) Calling-Station-Id attribute in all Authentication and Accounting packets for the context in which the feature is enabled.

The attribute contains a string that includes the SMS device hostname, a port description, and a circuit identification. These elements are separated in the string by the character configured with the **separator** *character* construct.

This command has no effect on virtual circuit sessions that come in via Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F). Those circuits can have a Calling-Station-Id attribute that is independent of this command.

Use the **no** form of this command to disable the sending of the Calling-Station-Id attribute.

Examples

The following example configures the context so that the Calling-Station-Id attribute is sent in Authentication and Accounting packets, using a slash as the separator character:

```
[local]RedBack(config-ctx)#radius attribute calling-station-id separator /
```

Related Commands

debug radius
radius attribute acct-session-id
radius attribute connect-info
radius attribute filter-id
radius attribute medium-type
radius attribute nas-ip-address
radius attribute non-rfc-242
radius attribute tunnel password

radius attribute connect-info

radius attribute connect-info profile-name

no radius attribute connect-info

Purpose

Specifies that ATM and Frame-Relay profile names are sent to the Remote Authentication Dial-In User Service (RADIUS) server via the Connect-Info attribute.

Command Mode

context configuration

Syntax Description

profile-name	Specifies that the information being provided to the RADIUS server consists of a profile name.

Default

Profile names are not sent to the RADIUS server.

Usage Guidelines

Use the **radius attribute connect-info** command to enable the sending of ATM and Frame-Relay profile names to the RADIUS server as part of the Connect-Info attribute. The Connect-Info attribute is used to describe the type of connection the subscriber uses. The type of connection is typically configured as part of the profile.

Use the **no** form of this command to disable the sending of profile names in the Connect-Info attribute.

Examples

The following example configures the SMS device to send ATM and Frame-Relay profile names to the RADIUS server:

```
[local]RedBack(config-ctx)#radius attribute connect-info profile-name
```

Related Commands

debug radius
radius attribute acct-session-id
radius attribute calling-station-id

radius attribute filter-id
radius attribute medium-type
radius attribute nas-ip-address
radius attribute non-rfc-242
radius attribute tunnel password

radius attribute filter-id

radius attribute filter-id direction {**in** | **out** | **both** | **none**}

default radius attribute filter-id

Purpose

Specifies the behavior of the Subscriber Management System (SMS) device when it receives a Remote Authentication Dial-In User Service (RADIUS) Filter-Id attribute that does not indicate a direction.

Command Mode

context configuration

Syntax Description

direction	Keyword preceding the specification of direction.
in	Applies the access control list on inbound packets.
out	Applies the access control list on outbound packets.
both	Applies the access control list on both inbound and outbound packets.
none	Ignores the Filter-Id attribute and does not apply the access control list in either direction.

Default

The SMS device ignores the Filter-Id attribute.

Usage Guidelines

Use the **radius attribute filter-id** command to configure the SMS device to handle all Filter-Id attributes that do not specify a direction. The SMS device can respond in one of four ways—by applying access control lists on the inbound direction, the outbound direction, both directions, or neither direction. The choice of behavior depends on the nature of the access control list involved and the type of data that is exchanged. For example, it may be appropriate to prevent subscribers from sending data to the Internet, or it may be appropriate to prevent data from reaching subscribers. This command is applied to all cases within the current context.

Use the **default** form of this command to reset the SMS device to ignore the Filter-Id attribute.

Examples

The following example configures the SMS device to handle missing RADIUS Filter-Id attributes by applying corresponding access control lists to inbound packets:

```
[local]RedBack(config-ctx)#aaa authentication subscriber radius
[local]RedBack(config-ctx)#radius attribute filter-id direction in
```

Related Commands

aaa authentication subscriber
debug radius
ip access-list
radius attribute acct-session-id
radius attribute calling-station-id
radius attribute connect-info
radius attribute medium-type
radius attribute nas-ip-address
radius attribute non-rfc-242
radius attribute tunnel password

radius attribute medium-type

radius attribute medium-type {**dsl** | **cable** | **wireless** | **satellite**}

{**no** | **default**} **radius attribute medium-type**

Purpose

Specifies the value that the Access Operating System (AOS) supplies for the Medium-Type vendor-specific attribute (VSA) in Remote Authentication Dial-In User Service (RADIUS) Access-Request and Accounting-Request packets.

Command Mode

Asynchronous Transfer Mode (ATM) profile configuration
Frame Relay profile configuration
port configuration

Syntax Description

dsl	Specifies that the value of the Medium-Type VSA is dsl.
cable	Specifies that the value of the Medium-Type VSA is cable.
wireless	Specifies that the value of the Medium-Type VSA is wireless.
satellite	Specifies that the value of the Medium-Type VSA is satellite.

Default

Sending of the Medium-Type attribute is disabled.

Usage Guidelines

Use the **radius attribute medium-type** command to specify the value that the AOS supplies for the Medium-Type VSA in RADIUS Access-Request and Accounting-Request packets.

For ATM and Frame Relay profiles, this command specifies the value of the Medium-Type attribute for any circuits that reference the profile.

For Ethernet ports, this command specifies the value of the Medium-Type attribute for any Point-to-Point Protocol over Ethernet (PPPoE) sessions that arrive at the SMS device over the port. This command does not apply to ports of types other than Ethernet.

Use the **no** or **default** form of this command to disable the sending of the attribute.

Note This command description also appears in Chapter 10, “Ethernet Port Commands,” Chapter 17, “ATM Commands,” and Chapter 18, “Frame Relay Commands.”

Examples

The following example creates the ATM profile named DSL-UBR in which the Medium-Type attribute is configured for dsl. If RADIUS Accounting is enabled, then the permanent virtual circuits (PVCs) in port 4/0 that reference this profile have Accounting packets with the Medium-Type attribute containing the value dsl. Similarly, attempts to authenticate the PPP user via RADIUS cause the attribute to be present in Access-Request packets:

```
[local]RedBack(config)#atm profile DSL-UBR
[local]RedBack(config-atmpro)#shaping ubr
[local]RedBack(config-atmpro)#radius attribute medium-type dsl
[local]RedBack(config-atmpro)#exit
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#atm pvc 0 1 through 100 profile DSL-UBR encapsulation ppp
[local]RedBack(config-pvc)#bind authentication chap pap
```

The following example configures the sessions that arrive over the specified Ethernet port to be associated with cable subscribers:

```
[local]RedBack(config)#port ethernet 3/0
[local]RedBack(config-port)#radius attribute medium-type cable
[local]RedBack(config-port)#encapsulation ppp over-ethernet
[local]RedBack(config-port)#bind authentication chap pap
```

Related Commands

aaa accounting
atm profile
debug radius
frame-relay profile
radius attribute acct-session-id
radius attribute calling-station-id
radius attribute connect-info
radius attribute filter-id
radius attribute nas-ip-address
radius attribute non-rfc-242
radius attribute tunnel password

radius attribute nas-ip-address

radius attribute nas-ip-address interface *if-name*

default radius attribute nas-ip-address interface *if-name*

Purpose

Adds the NAS-IP-Address attribute to Remote Authentication Dial-In User Service (RADIUS) request packets sent by the Subscriber Management System (SMS) device.

Command Mode

context configuration

Syntax Description

interface *if-name*	Name of the interface whose IP address is to be sent as the NAS-IP-Address attribute in the RADIUS request packet.

Default

The NAS-IP-Address attribute is not sent.

Usage Guidelines

Use the **radius attribute nas-ip-address** command to add the NAS-IP-Address attribute to every RADIUS request packet originating from a context.

Use the **default** form of this command to reset the SMS device behavior so that the NAS-IP-Address attribute is not sent.

Examples

The following example sends the configured IP address for interface `ether21` as the NAS-IP-Address attribute in every RADIUS request packet sent by the SMS device:

```
[local]RedBack(config-ctx)#radius attribute nas-ip-address interface ether21
```

Related Commands

debug radius
radius attribute acct-session-id
radius attribute calling-station-id
radius attribute connect-info

radius attribute filter-id
radius attribute medium-type
radius attribute non-rfc-242
radius attribute tunnel password

radius attribute non-rfc-242

radius attribute non-rfc-242

no radius attribute non-rfc-242

Purpose

Specifies that subscriber level access control lists can be loaded from a Remote Authentication Dial-In User Service (RADIUS) server via the Ascend-Data-Filter attribute.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

The ability to download subscriber level access control lists is disabled.

Usage Guidelines

Use the **radius attribute non-rfc-242** command to enable the ability to load subscriber level access control lists from the RADIUS server via the Ascend-Data-Filter attribute.

Use the **no** form of this command to disable the ability to download subscriber level access control lists.

Examples

The following example enables the ability to load subscriber level access control lists from the RADIUS server.

```
[local]RedBack(config-ctx)#radius attribute non-rfc-242
```

Related Commands

debug radius
radius attribute acct-session-id
radius attribute calling-station-id
radius attribute connect-info
radius attribute filter-id

radius attribute medium-type
radius attribute nas-ip-address
radius attribute tunnel password

radius attribute tunnel password

radius attribute tunnel password encrypt

[**no** | **default**] **radius attribute tunnel password**

Purpose

Specifies whether or not the Subscriber Management System (SMS) device expects the Tunnel-Password attribute to be encrypted in Remote Authentication Dial-In User Service (RADIUS) Access-Response packets.

Command Mode

context configuration

Syntax Description

encrypt	Specifies that the SMS device expects the Tunnel-Password attribute to be encrypted.

Default

The SMS device expects no encryption on the Tunnel-Password attribute.

Usage Guidelines

Use the **radius attribute tunnel password** command to specify that the SMS device should expect the Tunnel-Password attribute to be encrypted in RADIUS Access-Response packets. When the Tunnel-Password attribute is not encrypted, it is sent in clear text.

For example, it is important to have the Tunnel-Password attribute encrypted when a RADIUS proxy forwards traffic through an unsecured segment of the network.

Use the **no** or **default** form of this command to reset the SMS device to the default behavior of not expecting password encryption.

Examples

The following example configures the SMS device not to expect encryption of the Tunnel-Password attribute in the `local` context, but to expect password encryption in the `retail` context:

```
[local]RedBack(config)#context local
[local]RedBack(config-ctx)#aaa authorization tunnel radius
[local]RedBack(config-ctx)#radius server 1.1.1.1 key MySecret
[local]RedBack(config-ctx)#default radius attribute tunnel password
```

```
[local]RedBack(config)#context retail
[local]RedBack(config-ctx)#aaa authorization tunnel radius
[local]RedBack(config-ctx)#radius server 2.2.2.2 key YourSecret
[local]RedBack(config-ctx)#radius attribute tunnel password encrypt
```

Related Commands

aaa authorization tunnel
debug radius
radius attribute acct-session-id
radius attribute calling-station-id
radius attribute connect-info
radius attribute filter-id
radius attribute medium-type
radius attribute nas-ip-address
radius attribute non-rfc-242

radius deadtime

radius deadtime *minutes*

default radius deadtime

Purpose

Specifies the interval after which the Subscriber Management System (SMS) device is to treat a non-responsive Remote Authentication Dial-In User Service (RADIUS) server as dead, and try to reach the server.

Command Mode

context configuration

Syntax Description

minutes	Deadtime interval in minutes. The range of values is 0 to 65,535; the default value is 5. The 0 value disables this feature.

Default

The SMS device waits five minutes before trying to reach a nonresponsive RADIUS server.

Usage Guidelines

Use the **radius deadtime** command to specify the interval after which the SMS device is to treat a nonresponsive RADIUS server as dead, and try to reach the server.

Use the **default** form of this command to reset the deadtime to five minutes.

Examples

The following example changes the deadtime to `10` minutes:

```
[local]RedBack(config-ctx)#radius deadtime 10
```

Related Commands

radius algorithm
radius max-outstanding
radius max-retries

radius server
radius strip-domain
radius timeout

radius max-outstanding

radius max-outstanding *requests*

{**no** | **default**} **radius max-outstanding**

Purpose

Configures the number of simultaneous outstanding requests that can be sent by the Subscriber Management System (SMS) device to Remote Authentication Dial-In User Service (RADIUS) servers.

Command Mode

context configuration

Syntax Description

requests	Number of simultaneous outstanding requests. The range of values is 1 to 256.

Default

The maximum number of allowable outstanding requests is 256.

Usage Guidelines

Use the **radius max-outstanding** command to configure the number of simultaneous outstanding requests the SMS device can send to a RADIUS server. Use this command if the server cannot handle the default of 256 requests. If you have specified a RADIUS accounting server, this command only applies to authentication requests; otherwise, it applies to both authentication and accounting requests.

Use the **no** or **default** form of this command to reset the maximum number of outstanding requests to 256.

Examples

The following example sets the number of simultaneous outstanding requests to `128`:

```
[local]RedBack(config-ctx)#radius max-outstanding 128
```

Related Commands

radius algorithm
radius deadtime
radius max-retries

radius server
radius strip-domain
radius timeout

radius max-retries

radius max-retries *retries*

default radius max-retries

Purpose

Configures the number of retransmissions by the Subscriber Management System (SMS) device if a Remote Authentication Dial-In User Service (RADIUS) does not send an acknowledgment.

Command Mode

context configuration

Syntax Description

retries	Number of times the SMS device is to retransmit a RADIUS accounting packet. The range of values is 1 to 2,147,483,647; the default is 3.

Default

The SMS device sends three retransmissions.

Usage Guidelines

Use the **radius max-retries** command to modify the retransmission behavior of the SMS device in the event that an acknowledgment is not received from a RADIUS server within the configured time.

If an acknowledgment is not received, each successive server is tried (wrapping from the last server to the first, if necessary) until the maximum number of retransmissions is reached.

Use the **default** form of this command to reset the number of retries to three.

Examples

The following example sets the retransmit value to 5:

```
[local]RedBack(config-ctx)#radius max-retries 5
```

The following example resets the retransmit value to the default:

```
[local]RedBack(config-ctx)#default radius max-retries
```

Related Commands

radius algorithm
radius deadtime
radius max-outstanding
radius server
radius strip-domain
radius timeout

radius server

radius server {*ip-address* | *hostname*} **key** *key* [**oldports** | **port** *udp-port*] [**max** [*requests*]]

no radius server {*ip-address* | *hostname*}

Purpose

Configures Remote Authentication Dial-In User Service (RADIUS) servers.

Command Mode

context configuration

Syntax Description

ip-address	IP address of the RADIUS server.
hostname	Hostname of the RADIUS server. The Domain Name System (DNS) must be enabled in order to use the *hostname* argument. See the “Usage Guidelines” section in this command description.
key *key*	Alphanumeric string indicating the authentication key that must be shared with the RADIUS server.
oldports	Designates the old RADIUS User Datagram Protocol (UDP) ports 1,645 and 1,646.
port *udp-port*	RADIUS accounting UDP port.The range of values is 1 to 65,536. If no port is specified, UDP port 1,812 is used as the default for authentication and port 1,813 for accounting.
max *requests*	Maximum number of outstanding requests that can be sent to this server. The range of values is 1 to 256; the default is 256. This overrides the value set with the **radius max-outstanding** command.

Default

There is no default RADIUS server. However, when one is configured without a port specification, UDP port 1,812 is used as the default for authentication and port 1,813 for accounting. When the **max** keyword is specified without a value, the default is 256.

Usage Guidelines

Use the **radius server** command to configure a RADIUS server. You can configure one server to perform both authentication and accounting using the **radius server** command. Or, you can configure a separate RADIUS accounting server using the **radius accounting server** command.

If you configure a RADIUS server or RADIUS accounting server in the local context, these servers perform authentication and accounting for the entire device. The Access Operating System (AOS) provides warnings if a context-specific authentication server is configured when global authentication is enabled.

You can only use the *hostname* argument if DNS has been enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode. See Chapter 28, "DNS Commands," for descriptions of these commands.

Use the **no** form of this command to delete a previously configured RADIUS server.

Examples

The following example defines a remote RADIUS server with IP address `10.2.3.4` and key `TopSecret`, using the default authentication and accounting ports of 1,812 and 1,813:

```
[local]RedBack(config-ctx)#radius server 10.2.3.4 key TopSecret
```

The following example defines a remote RADIUS server with an IP address of `10.3.3.3` and the key `NotTooObvious` using ports `4444` and `4445` for authentication and accounting, respectively:

```
[local]RedBack(config-ctx)#radius server 10.3.3.3 key NotTooObvious port 4444
```

Related Commands

aaa accounting
aaa authentication subscriber
ip domain-lookup
ip domain-name
ip name-servers
radius algorithm
radius deadtime
radius max-outstanding
radius max-retries
radius strip-domain
radius timeout

radius strip-domain

radius strip-domain

no radius strip-domain

Purpose

Strips the domain portion of a structured username before relaying an authentication request to a Remote Authentication Dial-In User Service (RADIUS) server.

Command Mode

context configuration

Syntax Description

This command has no keywords or arguments.

Default

The entire username, including the domain name, is sent to the RADIUS server.

Usage Guidelines

Use the **radius strip-domain** command to specify that the domain portion of a structured username is to be removed before sending the username to a RADIUS server for authentication. The domain portion can be stripped, even if custom structured username formats have been defined using the **aaa username-format** command.

Use the **no** form of this command to disable stripping of the domain portion of the structured username.

Examples

The following example prevents the domain portion of the structured username from being sent to the RADIUS server for authentication:

```
[local]RedBack(config-ctx)#radius strip-domain
```

The following example resets the RADIUS strip-domain value to the default, thereby sending the entire structured username string to the RADIUS server:

```
[local]RedBack(config-ctx)#no radius strip-domain
```

Related Commands

aaa username-format
radius algorithm
radius deadtime
radius max-outstanding
radius max-retries
radius server
radius timeout

radius timeout

radius timeout *seconds*

default radius timeout

Purpose

Sets the maximum time the Subscriber Management System (SMS) device is to wait for a response from a Remote Authentication Dial-In User Service (RADIUS) server before assuming that a packet is lost.

Command Mode

context configuration

Syntax Description

seconds	Timeout period in seconds. The range of values is 1 to 2,147,483,647; the default is 10.

Default

The timeout interval is 10 seconds.

Usage Guidelines

Use the **radius timeout** command to set the maximum time the SMS device is to wait for a response from a RADIUS server before assuming that a packet is lost.

Use the **default** form of the command to return to the default value of 10 seconds.

Examples

The following example sets the radius timeout to `30` seconds:

```
[local]RedBack(config-ctx)#radius timeout 30
```

Related Commands

aaa accounting
aaa authentication subscriber
radius deadtime
radius max-outstanding

radius max-retries
radius server
radius strip-domain

show radius counters

show radius counters

Purpose

Displays counters for Remote Authentication Dial-In User Service (RADIUS) access and accounting messages for the current context.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None.

Usage Guidelines

Use the **show radius counters** command to display the RADIUS message counters for the current context shown in Table 41-1:

Table 41-1 RADIUS Message Counters

Field	Description
Access Messages–Requests sent	Number of access request messages sent
Access Messages–Accepts received	Number of access accept messages received
Access Messages–Rejects received	Number of access reject messages received
Access Messages–Requests retry	Number of access request retry messages sent
Accounting Messages–Requests sent	Number of accounting request messages sent
Accounting Messages–Responses received	Number of accounting request message responses received
Accounting Messages–Requests retry	Number of accounting request retry messages sent

Examples

The following example shows sample output from the **show radius counters** command:

```
[local]RedBack>show radius counters

Access Messages:                Accounting Messages
  Requests sent: 3                Requests sent: 100
  Accepts received: 3             Responses received: 100
  Rejects received: 0             Requests retry: 0
  Requests retry: 0
```

Related Commands

debug radius

Part 12

System Management

System Monitoring and Testing Commands

This chapter describes general system-wide monitoring and testing tasks, such as displaying system memory and processes, displaying all system hardware, testing IP connectivity, and enabling debugging messages for all IP packets.

This chapter describes general system **show** and **debug** commands. For information on **show** and **debug** commands that are specific to a feature, interfaces, subscribers, ports, or circuits, see the appropriate chapter in this guide. For example, to find out how to display or debug OSPF parameters, see Chapter 33, "OSPF Commands."

For overview information and a description of the tasks used to monitor and test system-wide parameters, see the "Monitoring and Testing System Parameters" chapter in the *Access Operating System (AOS) Configuration Guide*.

clear administrator

clear administrator *name*

Purpose

Ends a Telnet session for an administrator or operator.

Command Mode

operator exec

Syntax Description

name	Administrator name (*admin@context*).

Default

None

Usage Guidelines

Use the **clear administrator** command to end a Telnet session for an administrator or operator. An administrator in the local context can end any administrator session. Administrators in any other context can only end sessions in their own context.

Examples

The following command ends the Telnet session for the operator or administrator named `user34` in the `local` context:

```
[local]RedBack>clear administrator user34@local
```

Related Commands

show administrators

clear circuit

clear circuit {*slot/port* {*vpi vci* [**through** *end-vci*] | [*hdlc-channel*] *dlci* [**through** *end-dlci*] | **all**} | **pppoe** {[*cm-index*-]*session-id* [**through** *end-session-id*] | **all**}}

Purpose

Clears active subscriber sessions on the specified circuits.

Command Mode

operator exec

Syntax Description

slot/port	Backplane slot number and port number of an Asynchronous Transfer Mode (ATM) or Frame Relay port.
vpi	Virtual path identifier (VPI) of the circuit. The range of values is 0 through 255.
vci	Virtual channel identifier (VCI) of the circuit. For ATM T1 I/O modules, the range of values is 1 to 1,023; for ATM DS-3 Version 1 I/O modules, the range of values is 1 to 2,047; for ATM OC-3 Version 1 I/O modules, the range of values is 1 to 4,095; for all ATM Version 2 I/O modules, the range of values is 1 to 65,535.
through *end-vci*	Optional. Last VCI when clearing a range of ATM circuits.
hdlc-channel	Name of the High-level Data Link Control (HDLC) channel in the case for a channelized DS-3 port. This argument is required for channelized DS-3 ports and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) of a configured Frame Relay permanent virtual circuit (PVC). The range of values is 16 through 991.
through *end-dlci*	Optional. Last DLCI when clearing a range of Frame Relay circuits.
pppoe {*session-id*}	Session ID of a particular Point-to-Point Protocol over Ethernet (PPPoE) circuits to be cleared.
cm-index-	Slot number of the Connection Manager (CM) module for the session. Specified only for hardware platforms that support CM modules.
through *end-session-id*	Optional. Last session ID when clearing a range of PPPoE sessions.
all	With the *slot/port* argument, specifies that all circuits on the specified slot and port are cleared. With the **pppoe** keyword, specifies that all PPPoE sessions are cleared.

Default

None

Usage Guidelines

Use the **clear circuit** command to clear active subscriber sessions on the specified circuit or circuits. This command is similar to the **clear subscriber** command; instead of specifying the username, you specify the circuit or PPPoE session ID. This is particularly useful when a subscriber may be using multiple circuits and there is only one that you want to clear.

Once circuits are cleared using this command, they remain in the unconfigured state until new activity is detected on them. At that time, the configuration is read from Remote Authentication Dial-In User Service (RADIUS) or from the default circuit specification, if one is configured. If any configuration changes were made, they are implemented at that time.

Note This command is also described in Chapter 9, "Common Port, Circuit, and Channel Commands."

Examples

The following example clears all active subscriber sessions on all circuits on slot/port `3/0`:

```
[local]RedBack>clear circuit 3/0 all
```

The following example clears a range of ATM circuits, VPI:VCI `10:10` through `10:40`:

```
[local]RedBack>clear circuit 5/0 10 10 through 40
```

Related Commands

clear subscriber
show atm pvc
show frame-relay pvc
show subscribers

clear fabric counters

clear fabric counters {*slot* | **all**}

Purpose

Clears the counters for the switch fabric on Connection Manager (CM) and System Manager (SM) modules.

Command Mode

administrator exec

Syntax Description

slot	Slot number of a particular CM or SM. Clears counters for the switch fabric on the CM or SM module in the specified slot.
all	Clears counters for the switch fabric on all CM and SM modules in the system.

Default

Counters for the switch fabric on all CM and SM modules are cleared.

Usage Guidelines

Use the **clear fabric counters** command to clear previous counter statistics (reset to 0). If no keyword is entered or if **all** is entered, counters for the switch fabric on all CM and SM modules are cleared. To clear counters for the switch fabric on a particular CM or SM, specify the CM or SM slot number.

Examples

The following example clears all counters for the switch fabric:

```
[local]RedBack#clear fabric counters
```

Related Commands

show fabric counters
fabric test

clear subscriber

clear subscriber *name*

Purpose

Clears a subscriber.

Command Mode

operator exec

Syntax Description

name Name of the subscriber to be cleared.

Default

None

Usage Guidelines

Use the **clear subscriber** command to clear a subscriber. The system checks if the subscriber is currently active and, if so clears the subscriber's circuit. In the case of Point-to-Point Protocol (PPP), the session is terminated and the subscriber is logged out. PPP then attempts to renegotiate and re-authenticate a new session with the remote peer on that circuit. In the case of RFC 1483-encapsulated and RFC 1490-encapsulated circuits, the circuit is brought down, and then back up, and an attempt is made to reauthenticate the subscriber that is bound to the circuit.

The command is useful when a subscriber's record has changed and you want the new parameters to take effect immediately, and also when a user account has been removed and you want to log the user off.

Note This command is also described in Chapter 8, "Subscriber Commands."

Examples

To clear the subscriber `dave@isp1`:

```
[local]RedBack>clear subscriber dave@isp1
```

Related Commands

clear circuit
show subscribers

debug all

debug all

no debug all

Purpose

Enables all available debugging options, except Asynchronous Transfer Mode (ATM) debugging.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use this **debug all** command to enable debugging of all system options, except for ATM debugging; use the **debug atm** command to enable ATM debugging.

Caution Debugging can severely affect system performance, particularly if debugging of all modules is enabled through the debug all command. Because of this, you will be prompted to confirm the operation. Type y to enable all debugging. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to turn off debugging of all system options.

Examples

The following example enables all debugging, then displays the debugging status:

```
[local]RedBack#debug all

   This may severely impact performance. Continue? [confirm]y
```

```
[local]RedBack#show debugging

ARP:
   ARP packet debugging is on
General IP:
   IP packet debugging is on
   IP host debugging is on
   IP route debugging is on
   IP interface debugging is on
   ICMP debugging is on
   IP inter-engine communication debugging is on
   TFTP debugging is on
   TELNET debugging is on
IP Routing:
   RIP protocol debugging is on
   IGMP protocol debugging is on
Bridge:
   Learned MAC address debugging is on
   Spanning tree debugging is on
AAA:
   Authentication debugging is on
   Authorization debugging is on
   Accounting debugging is on
RADIUS:
   Authentication debugging is on
   Authorization debugging is on
   Accounting debugging is on
   RADIUS packet debugging is on
   RADIUS attribute debugging is on
DHCP:
   DHCP packet debugging is on
PPP:
   Authentication debugging is on
   FSM-call debugging is on
   FSM state-change debugging is on
   IPCP protocol debugging is on
   LCP debugging is on
   Negotiation debugging is on
   Packet debugging is on
   Phase debugging is on
L2TP:
   Window debugging is on
   Tunnel state-change debugging is on
   Session state-change debugging is on
   Tunnel setup debugging is on
   Session setup debugging is on
   AAA debugging is on
   Packet debugging is on
PPPOE:
   Discovery debugging is on
   Virtual Circuit debugging is on
```

```
Slot Manager:
   Slot manager debugging is on
Port Manager:
   Port manager debugging is on
Circuit Manager:
   Circuit manager debugging is on
Frame Relay:
   Frame Relay packet debugging is on
   LMI packet debugging is on for all Frame Relay ports
```

Related Commands

debug atm
logging console
show debugging
show log
terminal monitor

debug ip all

debug ip all

no debug ip all

Purpose

Enables the logging of IP debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip all** command to enables the logging of IP debugging messages. When debugging is enabled, all IP-related messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

To turn on debug logging for all IP features, enter the following command:

```
[local]RedBack#debug ip all
```

Related Commands

logging console
show debugging
terminal monitor

debug ip ce-fe

debug ip ce-fe

no debug ip ce-fe

Purpose

Enables the logging of Control Engine (CE) and Forwarding Engine (FE) module debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip ce-fe** command to enable the logging of CE and FE module debugging messages. You can use the **logging console** or **terminal monitor** command to display messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables debug logging for CE and FE modules:

```
[local]RedBack#debug ip ce-fe
```

Related Commands

logging console
show fe stats
terminal monitor

debug ip host

debug ip host

no debug ip host

Purpose

Enables the logging of IP host debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Host debugging is disabled.

Usage Guidelines

Use the **debug ip host** command to enable the logging of host debugging messages.

When debugging is enabled, host messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable host debugging.

Examples

The following example enables debug logging for IP hosts:

```
[local]RedBack#debug ip host
```

Related Commands

logging console
ping
show debugging
terminal monitor
show tech

debug ip icmp

debug ip icmp

no debug ip icmp

Purpose

Enables the logging of IP Internet Control Message Protocol (ICMP) debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip icmp** command to enable the logging of ICMP debugging messages. ICMP router discovery messages enable hosts to find routers. ICMP Redirect messages provide information on the best router to use to reach a particular destination. ICMP Echo and Echo Reply (ping) messages determine whether a router or host is reachable. ICMP error messages aid in troubleshooting by helping determine which packets are causing problems.

When debugging is enabled, ICMP messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable ICMP debugging.

Examples

The following example enables debug logging for ICMP:

```
[local]RedBack#debug ip icmp
```

Related Commands

logging console
ping
show debugging
terminal monitor
show tech

debug ip packet

debug ip packet

no debug ip packet

Purpose

Enables the logging of IP packet debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip packet** command to enable the logging of IP packet debugging messages.

When you enable the **debug ip packet** command, the log event output filter for syslog and telnet sessions do not allow any of the debug ip packet events. This is to avoid a situation where a packet is sent, causing an event to be logged, causing a packet to be sent, and so on in an endless loop.

You can use the **logging console** or **terminal monitor** command to display messages in real time, except for the following six events which are filtered out:

- EVNT_IP_RX_HDR—received IP packet
- EVNT_IP_TX_HDR—sent IP header
- EVNT_IP_RX_TCP_HDR—received TCP packet
- EVNT_IP_TX_TCP_HDR—sent TCP header
- EVNT_IP_RX_UDP_HDR—received UDP packet
- EVNT_IP_TX_UDP_HDR—sent UDP header

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable IP packet debugging.

Examples

The following example enables debug logging for all IP packets:

```
[local]RedBack#debug ip packet
```

Related Commands

logging console
show debugging
terminal monitor

debug ip sm-cm

debug ip sm-cm

no debug ip sm-cm

Purpose

Enables the logging of System Manager (SM) and Connection Manager (CM) module debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

Debugging is disabled.

Usage Guidelines

Use the **debug ip sm-cm** command to enable the logging of SM and CM module debugging messages. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable debugging.

Examples

The following example enables debug logging for SM and CM modules:

```
[local]RedBack#debug ip sm-cm
```

Related Commands

logging console
show cm stats
show cm table
show debugging
terminal monitor

debug ip tcp

debug ip tcp

no debug ip tcp

Purpose

Enables the logging of IP Transmission Control Protocol (TCP) debugging messages.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

TCP debugging is disabled.

Usage Guidelines

Use the **debug ip tcp** command to enable the logging of TCP debugging messages.

When debugging is enabled, TCP messages are logged. You can use the **logging console** or **terminal monitor** command to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable TCP debugging.

Examples

The following example enables debug logging for TCP:

```
[local]RedBack#debug ip tcp
```

Related Commands

logging console
ping
show debugging
terminal monitor
show tech

fabric test

fabric test

Purpose

Tests the fabric switch using all Connection Manager (CM) and System Manager (SM) modules in the system.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **fabric test** command to test the fabric switch using all CM and SM modules in the system. Possible results are passed, failed, and unknown. Internal and external tests are run at several times: at system bootup, when this command is issued, and if the system determines that it must switch to an untested timing module. Newly inserted CM modules can perform only external tests on the timing module that is currently used by the system. Results for an untested timing module is tagged as unknown.

Use the **show fabric table** command to view test results.

Examples

The following example tests the fabric using all SMs and CMs in the system:

```
[local]RedBack>fabric test

Performing fabric tests...
```

Related Commands

show fabric table

ping

ping {*ip-address* | *hostname*} [*number-of-packets*] [**interface** *name* | **src** *ip-address*] [**pattern** *hex-pattern*] [**size** *bytes*] [**timeout** *seconds*]

Purpose

Tests the reachability of a host.

Command Mode

operator exec

Syntax Description

hostname	Name of the host. Domain Name System (DNS) must be enabled.
ip-address	IP address of the host.
number-of-packets	Optional. Number of ping packets to send. The range of values is 1 to 10,000; the default is 5.
interface *name*	Optional. Name of the interface from which ping packets are sourced. Uses the primary address of the interface, which must be in the UP state, as the source of ping packets.
src *ip-address*	Optional. IP source address of the ping packets. An interface with this IP address must exist.
pattern *hex-pattern*	Optional. Hex pattern to fill in Internet Control Message Protocol (ICMP) packets. The range of values is 0x0 to 0xffffffff.
size *bytes*	Optional. Size, in bytes, of the IP datagram. The range of values is 40 to 18432; the default is 100.
timeout *seconds*	Optional. Amount of time, in seconds, that the system waits for a response for each ping packet. The range of value is 1 to 100; the default is 2.

Default

This command sends five 100-byte packets to the specified host, using a timeout value of two seconds.

Usage Guidelines

Use the **ping** command to test the reachability of a host.

You can only use the *hostname* argument if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode. See Chapter 28, “DNS Commands.”

Press **Ctrl+C** to stop a ping test.

The **ping** and **traceroute** commands can have vastly different output, depending on the context in which the commands are executed. In particular, an IP address that can be reached by the **ping** or **traceroute** command in one context might not be reachable from another context. Use the **context** administrator exec mode command to switch between contexts.

Examples

The following example sends 5 ping packets to host `10.1.1.1`:

```
[local]RedBack>ping 10.1.1.1

Sending 5, 100-byte ICMP echoes to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

The following example sends 3 ping packets, each of size `1000` bytes to host `10.1.1.1`:

```
[local]RedBack>ping 10.1.1.1 3 size 1000

Sending 3, 1000-byte ICMP echoes to 10.1.1.1, timeout is 2 seconds:
!!!
Success rate is 100 percent (3/3), round-trip min/avg/max = 0/1/2 ms
```

Related Commands

ip domain-lookup
ip domain-name
ip name-servers
show tech

show administrators

show administrators [**active** [*name*]]

Purpose

Displays information about the active administrator and operator sessions on the system.

Command Mode

operator exec

Syntax Description

active	Optional. Displays a summary of the output that includes only administrators in the current context.
name	Optional. Summary information for the specified administrator.

Default

Displays all active administrator and operator sessions.

Usage Guidelines

Use the **show administrators** command to display a list of administrators and operators active in all contexts. Use the **active** keyword to display summary information about administrators in the current context. Use the *name* argument to include only information about the specified administrator.

In the display, administrator sessions are distinguished from operator sessions by the asterisk (*) in front of the corresponding name. In addition, an asterisk (*) in front of the terminal name indicates the session.

Examples

The example below shows the output from the **show administrators** command. The asterisk in the first column (preceding the `TTY` column) indicates that the administrator connected to the `console` port executed the command. The context listed is the one in which the operator or administrator was authenticated.

```
[local]RedBack>show administrators

   TTY       ADMINISTRATOR       CONTEXT       START TIME
   ------------------------------------------------------------------------
*  console   * admin@local       local         TUE JUN 23 14:11:00 1999
   tty1        oper@local        local         TUE JUN 23 12:38:10 1999
   tty2      * admin2@newcontext local         TUE JUN 23 13:49:21 1999
```

The following example shows the output from the **show administrators active** command:

```
[local]RedBack>show administrators active

administrator admin@local
```

Related Commands

clear administrator

show cm stats

show cm stats *slot*

Purpose

Displays Connection Manager (CM) module statistics.

Command Mode

operator exec

Syntax Description

slot	Slot number of the CM module.

Default

None

Usage Guidelines

Use the **show cm stats** command to display CM statistics.

Examples

The following example displays statistics for a CM in slot 0:

```
[local]RedBack#sh cm stats 0

--- Global Stats ---
rounds:               289,572,583       ticks:                108,562
pkts_rcvd:                     34       free_buffers:               0
buf_alloc_fails:                0       bad_l2_protocol:            0
cm_pkt_rcvs:                    0       sm_pkt_xmts:                0
bogus_cct_xmts:                 0       sm_pkt_rcv_ring_full:       0
l2_runt_pkts:                   0       pppoe_runt_pkts:            0


--- IP Stats ---
ip_pkts_rcvd:                   0       ip_pkts_xmtd:             692
ip_ttl_expired:                 0       no_ip_route:                0
bad_ip_xsums:                   0       rcv_bad_ip_ver:             0
arp_resource_errs:              0       no_nxthop_host:             0
arp_decaps_drops:               0       ip_acl_inb_drops:           0
```

```
llc_too_small:                  0       llc_too_large:              0
ip_acl_outb_drops:              0       ip_cct_acl_inb_drops:       0
ip_cct_acl_outb_drops:          0       other_ip_errors:            0
invalid_ip_srcs:                0       invalid_ip_dsts:            0
ip_pkts_fragmented:             0       ip_fragments_xmtd:          0
ip_dont_fragment_drops:         0       ip_fragment_runt_pkts:      0
CM reassy's completed:          0       CM mem resource err:        0
CM reassy's canceled:           0       CM reassy buf limit:        0
ip_runt_pkts:                   0       not_resolved:               0
l2_len_<_min_hlen:              0       ip_hlen_too_short:          0
ip_pkt_len_too_short:           0       l2_len_<_ip_len:            0
ip_mcast_pkts_rcvd:             0       ip_mcast_pkts_xmtd:         0
mcast_pkts_fragmented:          0       mcast_fragments_xmtd:       0
l2_mcast_drop:                  0


--- L2TP Stats ---
l2tp_pkts_rcvd:                 0       l2tp_sm_dlvrs:              0
l2tp_lns_dlvrs:                 0       l2tp_lac_dlvrs:             0
l2tp_lns_bypass_dlvrs:          0       l2tp_lac_bypass_dlvrs:      0
l2tp_ip_xmits:                  0       l2tp_pvc_xmits:             0
l2tp_ip_errs:                   0       last_l2tp_ip_err:           0
l2tp_no_tunnel:                 0       l2tp_no_session:            0
l2tp_flow_ctl:                  0       l2tp_len_err:               0
l2tp_no_tid:                    0       l2tp_no_t_bit:              0
l2tp_police_drops:              0       l2tp_rate_drops:            0


--- Bridge Packet Filtering Stats ---
acl_inb_drops:                  0       acl_outb_drops:             0
cct_acl_inb_drops:              0       cct_acl_outb_drops:         0
other_acl_inb_errors:           0       other_acl_outb_errors:      0
q8021_no_config:                0
[local]RedBack#
```

Table 42-1 (global statistics), Table 42-2 (IP statistics), Table 42-3 (L2TP statistics), and Table 42-4 (bridge packet filtering statistics) describe the output fields for the **show cm stats** command:

Table 42-1 Global Stats

Display Field	Description
rounds	Number of times the CM module has cycled through its main loop; indicates how busy the CM module is (smaller increments indicate that the CM module is busier)
ticks	Timing clock for noncritical intervals on the CM module (increments once every 16.67 ms)
pkts_rcvd	Number of packets received by the CM module; excludes packets from the SM and those packets for which no PVC exists
free_buffers	Not used
buf_alloc_fails	Number of times the CM module has failed when trying to allocate a buffer to send or receive a packet

Table 42-1 Global Stats

Display Field	Description
bad_l2_protocol	Number of packets discarded by the CM module due to an invalid layer 2 protocol header
cm_pkt_rcvs	Number of data packets transferred from the CM module to the SM module
sm_pkt_xmts	Number of data packets received by the CM module from the SM module
bogus_cct_xmts	Number of packets transmitted via a port that is no longer configured
sm_pkt_rcv_ring_full	Number of packets destined to the SM dropped by the CM module due to congestion between the SM module and the CM module
l2_runt_pkts	Number of packets detected as too small while processing layer 2 protocol headers.
pppoe_runt_pkts	Number of PPPoE packets with length too small.

Table 42-2 IP Stats

Display Field	Description
ip_pkts_rcvd	Number of IP packets received by the CM module
ip_pkts_xmtd	Number of IP packets transmitted by the CM module
ip_ttl_expired	Number of IP packets discarded by the CM due to expired time-to-live
no_ip_route	Number of IP packets discarded by the CM module because it had no route to the destination
bad_ip_xsums	Number of IP packets discarded by the CM module due to a bad IP checksum
rcv_bad_ip_ver	Number of IP packets discarded by the CM module due to an invalid IP version
arp_resource_errs	Number of IP packets discarded by the CM module due to a lack of resources needed to resolve the destination address
no_nxthop_host	Number of IP packets discarded by the CM module because the next hop was unreachable
arp_decaps_drops	Number of IP packets discarded by the CM module due to an unrecognized encapsulation
ip_acl_inb_drops	Number of IP packets discarded by the CM module due to an inbound IP access list restriction
llc_too_small	Number of IP packets discarded by the CM module due to the packet being too small
llc_too_large	Number of IP packets discarded by the CM module due to the packet size exceeding the frame size
ip_acl_outb_drops	Number of IP packets discarded by the CM module due to an outbound IP access list restriction
ip_cct_acl_inb_drops	Number of IP packets discarded by the CM due to an inbound circuit-level access list restriction.
ip_cct_acl_outb_drops	Number of IP packets discarded by the CM module due to an outbound circuit-level access list restriction
other_ip_errors	Number of IP packets discarded by the CM module due to an unclassified error.
invalid_ip_srcs	Number of IP packets discarded by the CM module due to an invalid source address

Table 42-2 IP Stats

Display Field	Description
invalid_ip_dsts	Number of IP packets discarded by the CM module due to an invalid destination address
ip_pkts_fragmented	Number of packets fragmented by the CM module
ip_fragments_xmtd	Number of fragments transmitted by the CM module
ip_dont_fragment_drops	Number of IP packets discarded by the CM because the packet was flagged as “don’t fragment,” but the packet size exceeded the MTU of the next hop interface module
ip_fragment_runt_pkts	Number of IP packets discarded by the CM module because the receive length was less than the length indicated in the packet.
CM reassy’s completed	Number of packet reassemblies completed.
CM mem resource err	Number of IP packets discarded by the CM module due to a lack of resources needed to reassemble the packet
CM reassy’s canceled	Number of IP packets discarded by the CM module due to a delay in receiving all the fragments
CM reassy buf limit	Not used
ip_runt_pkts	Number of IP runts discarded by the CM module
not_resolved	Number of IP packets discarded by the CM module because it could not resolve the destination address
l2_len_<_min_hlen	Number of IP packets discarded by the CM module due to a packet length less than the minimum header length.
ip_hlen_too_short	Number of IP packets discarded by the CM module due to an IP header length less than the required minimum for an IP packet
ip_pkt_len_too_short	Number of IP packets discarded by the CM due to an IP packet length value less than the minimum for an IP packet
l2_len_<_ip_len	Number of IP packets discarded by the CM module due to the frame length being smaller than the IP packet length
ip_mcast_pkts_rcvd	Number of IP multicast packets received by the CM module
ip_mcast_pkts_xmtd	Number of IP multicast packets transmitted by the CM module
mcast_pkts_fragmented	Number of IP multicast packets fragmented by the CM module
mcast_fragments_xmtd	Number of IP multicast fragments transmitted by the CM module
l2_mcast_drop	Number of layer 2 multicast packets dropped by the CM module

Table 42-3 L2TP Stats

Display Field	Description
l2tp_pkts_rcvd	Number of L2TP and L2F data and control packets received
l2tp_cm_dlvrs	Number of L2TP and L2F control packets received
l2tp_lns_dlvrs	Number of L2TP and L2F data packets received at the LNS or HG
l2tp_lac_dlvrs	Number of L2TP and L2F data packets received at the LAC or NAS
l2tp_lns_bypass_dlvrs	Number of L2TP and L2F data packets received at the LNS or HG end of a tunnel switch

Table 42-3 L2TP Stats

Display Field	Description
l2tp_lac_bypass_dlvrs	Number of L2TP and L2F data packets received at the LAC or NAS end of a tunnel switch
l2tp_ip_xmits	Number of L2TP and L2F data packets transmitted over UDP/IP
l2tp_pvc_xmits	Number of L2TP and L2F data packets forwarded over PVCs
l2tp_ip_errs	Number of transmit failures for L2TP and L2F data packets over UDP/IP
last_l2tp_ip_err	Error code corresponding to the last failure to transmit a L2TP/L2F data packet over UDP/IP
l2tp_no_tunnel	Number of L2TP and L2F data packets dropped due to an invalid tunnel ID
l2tp_no_session	Number of L2TP and L2F data packets dropped due to an invalid session ID
l2tp_flow_ctl	Number of L2TP and L2F data packets dropped due to a full session-level window
l2tp_len_err	Number of L2TP and L2F data or control packets dropped due to a length-too-small error
l2tp_no_tid	Number of L2TP and L2F data packets with a zero tunnel ID
l2tp_no_t_bit	Number of L2TP and L2F data packets with a session ID of zero, but not marked as a control packet
l2tp_police_drops	Number of L2TP and L2F data packets dropped due to tunnel-level policing
l2tp_rate_drops	Number of L2TP and L2F data packets dropped due to tunnel-level rate-limiting

Table 42-4 Bridge Packet Filtering Stats

Display Field	Description
acl_inb_drops	Number of packets dropped by the CM module due to an inbound access list restriction
acl_outb_drops	Number of packets dropped by the CM module due to an outbound access list restriction
cct_acl_inb_drops	Number of packets dropped by the CM module due to an inbound circuit-level access list restriction
cct_acl_outb_drops	Number of packets dropped by the CM module due to an outbound circuit-level access list restriction
other_acl_inb_errors	Number of packets dropped by the CM module due to an unknown error during inbound access list processing
other_acl_outb_errors	Number of packets dropped by the CM module due to an unknown error during outbound access list processing
q8021_no_config	Number of packets with 802.1q Ethertype because of no ATM circuit bound to the port via the **bind dot1q** command

Related Commands

show cm table

show cm table

show cm table

Purpose

Displays the state of all Connection Manager (CM) modules in the Subscriber Management System (SMS) device.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show cm table** command to display the state of all CM modules.

The CM states are described in Table 42-5:

Table 42-5 CM Module States

CM State	Description
PRESENT	A CM module is present, but is not initialized.
IMAGE_LOADING	The CM module executable is being loaded.
BOOTING	The CM module is initializing.
IO DISCOVERY	The CM module is determining which I/O modules are present.
CFG_LOAD	The CM module is synchronizing its configuration with the System Manager (SM) module.
STEADY	The CM module has completed initialization and is running.
DUMPING	The CM module is dumping its log information to the SM module.

Examples

In the following example, the system has two CM modules and both have completed initialization and are running:

```
[local]RedBack#show cm table

CM #     State
----------------------------
0        STEADY
1        STEADY
```

Related Commands

show cm stats

show debugging

show debugging

Purpose

Displays which debugging options are currently enabled.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show debugging** command to display the debugging options that are currently enabled.

Examples

The following shows sample output from the **show debugging** command:

```
[local]RedBack>show debugging

ARP:
   ARP packet debugging is on
General IP:
   IP packet debugging is on
   IP host debugging is on
   IP route debugging is on
   IP interface debugging is on
   ICMP debugging is on
   IP inter-engine communication debugging is on
   TFTP debugging is on
   TELNET debugging is on
IP Routing:
   RIP protocol debugging is on
```

Related Commands

all **debug** commands

show diag

show diag [**all** | **backplane** | **ce** | **cm** [*slot*] | **fabric** | **fe** | **midplane** | **power** | *slot*/*port* | **sm** [*slot*] | **timing**] [**err**] [**long**]

Purpose

Displays the results of power-on diagnostic tests.

Command Mode

operator exec

Syntax Description

all	Optional. Displays results of all power-on diagnostic tests.
backplane	Optional. Displays backplane power-on diagnostics results.
ce	Optional. Displays Control Engine (CE) module power-on diagnostics results.
cm [*slot*]	Optional. Displays Connection Manager (CM) module power-on diagnostics results. If the **cm** keyword is entered without a slot number, results for all CM modules in the system are displayed. If *slot* argument is used, results for only the CM module in the specified slot is displayed.
fabric	Optional. Displays switch fabric power-on diagnostics results.
fe	Optional. Displays Forwarding Engine (FE) module power-on diagnostics results.
midplane	Optional. Displays midplane power-on diagnostics results.
power	Optional. Displays power supply diagnostics results.
slot/*port*	Optional. Power-on diagnostics results for the specified slot and port.
sm [*slot*]	Optional. System Manager (SM) module power-on diagnostics results. If the **sm** keyword is entered without a slot number, results for all SM modules in the system are displayed. If the *slot* argument is used, results for only the SM module in the specified slot is displayed.
timing	Optional. Displays timing module power-on diagnostics results.
err	Optional. Displays the power-on diagnostics error log.
long	Optional. Long form output. Provides a list of the tests executed and their results. If this keyword is used, the display of the error log is automatically enabled.

Default

Displays a summary of the results for all power-on diagnostic tests.

Usage Guidelines

Use the **show diag** command to display the results of power-on diagnostic tests. When no keywords or arguments are used, a summary of the results for all power-on diagnostic tests is displayed. To filter output, use an optional keyword or argument. Used alone, together, or with any keyword or argument, **long** displays the results of each type of diagnostic test run, while **err** displays an error log.

Note Keywords used with this command vary according to the platform on which the Redback Access Operating System (AOS) is running. If a particular keyword, for example, **cm**, is used on a platform that supports, for example, an FE instead, the system will interpret the **cm** keyword as **fe**.

Examples

The following example is based on a product platform that supports the FE module:

```
[local]RedBack>show diag

Module PCI_CFG MASTER_REG MASTER_MEM EEPROM PHY_REG PHY_MEM PRES_REG SERV_REG  LB
BKPL                                  PASS
AC PS2                                PASS
  0/0    PASS
  4/0    PASS      PASS        PASS      PASS     PASS     PASS     PASS     PASS     PASS
  4/1    PASS      PASS        PASS      PASS     PASS     PASS     PASS     PASS     PASS
  5/0    PASS      PASS        PASS      PASS     PASS     PASS     PASS     PASS     PASS
  5/1    PASS      PASS        PASS      PASS     PASS     PASS     PASS     PASS     PASS
  6/0    PASS      PASS                  PASS     PASS              PASS     PASS     PASS
  6/1    PASS      PASS                  PASS     PASS              PASS     PASS     PASS
  7/0    PASS      PASS                  PASS     PASS              PASS     PASS     PASS
  7/1    PASS      PASS                  PASS     PASS              PASS     PASS     PASS

               FE_FPGA    FE_EEPROM  FE_SRAM   FE_SRAM_HI     FE_TAG_SRAM     FE_TAG
8M FE 1 PROC    PASS       PASS       PASS       PASS            PASS
```

The following example is based on a product platform that supports CM and SM modules:

```
[local]RedBack>show diag

 HW Type          Location          POD Status
 -------          --------          ----------
MIDPLANE                           Passed all tests
FABRIC            a                Passed all tests
FABRIC            b                Passed all tests
FABRIC            c                Passed all tests
FABRIC            d                No tests executed
TIMING            5                Passed all tests
CM                0                Passed all tests
 ENET            0/0               Passed all tests
 ENET            0/1               Passed all tests
 CCDS3           1/0               No tests executed
 CCDS3           1/1               No tests executed
SM                2                Passed all tests
 ENET            4/0               Passed all tests
CM               7                 Passed all tests
 ATDS3          14/0               FAILED
 ATDS3          14/1               Passed all tests
```

The following example displays diagnostics results for the module in slot 14 on port 0:

```
[local]RedBack>show diag 14/0

 HW Type    Location     POD Status
 -------    --------     ----------
 ATDS3      14/0         FAILED
```

The following example displays errors along with the diagnostics results for the module in slot 14 on port 0:

```
[local]RedBack>show diag 14/0 err

 HW Type    Location     POD Status
 -------    --------     ----------
 ATDS3      14/0         FAILED

MARCH_B_MEMTEST_FAIL_2:  ADDR: 0x4810348c  Exp: 0x1278df43  Got: 0x3278df43
```

The following example displays diagnostics results for all CMs in the system:

```
[local]RedBack>show diag cm

 HW Type    Location    POD Status
--------    --------    -----------
CM          0           Passed all tests
CM          7           Passed all tests
```

The following example displays, in long form, a list of results for each type of diagnostic test performed on all CMs in the system:

```
[local]RedBack>show diag cm long

CM-0:
    Passed SDRAM Test.
    Passed CSR Register Test.
    Passed 21154 Bridge Test.
    Passed 8240 Mailbox Test.
CM-7:
    Passed SDRAM Test.
    Passed CSR Register Test.
    Passed 21154 Bridge Test.
    Passed 8240 Mailbox Test.
```

Related Commands

show hardware

show envmon

show envmon

Purpose

Displays environmental monitoring status information.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show envmon** command to display environmental monitor status, including fan and power supply failures.

Examples

The following example shows sample output from the **show envmon** command:

```
[local]RedBack>show envmon

No environmental monitor failures detected.
```

Related Commands

show diag

show fabric counters

show fabric counters [*slot* | **all**]

Purpose

Displays information about the switch fabric on Connection Manager (CM) and System Manager (SM) modules.

Command Mode

operator exec

Syntax Description

slot	Optional. Displays information about the switch fabric on the specified slot number of a CM or SM module.
all	Optional. Displays information the switch fabric on all CM and SM modules in the system.

Default

None

Usage Guidelines

Use the **show fabric counters** command to displays information about the switch fabric on CM and SM modules. If you use the *slot* argument, information specific to the CM or SM in the specified slot is displayed. If no keyword or argument is specified, the system provides total sums that represent the number of counters and errors for the switch fabric on all CM and SM modules in the system. When the **all** keyword is used, detailed information for each CM and SM module configured in the system is displayed in sequential order.

Examples

The following provides sample output for this command:

```
[local]RedBack#show fabric counters 1

THU JAN 06 21:02:32 2000
Slot   1 Fabric info:

last cleared:   never
Fabric Slice                  A         B         C         D
-------------------------------------------------------------------
status                        Active    Active    Active    Empty

receive slice link error      0         0         0         0
receive slice checksum error  0         0         0         0
transmit slice link error     0         0         0         0

Receive Counter:
bits per second                = 0
framelets per second           = 2
packets per second             = 2
max bits per second            = 128
max framelets per second       = 31
max packets per second         = 31
total framelets CRC errors(LSB) = 0
total framelets CRC errors(MSB) = 0
total number of framelets      = 0
total number of packets        = 0

Transmit Counter:
bits per second                = 1984
framelets per second           = 2
packets per second             = 2
max bits per second            = 18208
max framelets per second       = 27
max packets per second         = 27
total number of framelets      = 0
total number of packets        = 0
```

Related Commands

clear fabric counters

show fabric table

show fabric table [**detail**]

Purpose

Displays the switch fabric test status.

Command Mode

operator exec

Syntax Description

detail	Optional. Provides details on the fabric switch status.

Default

None

Usage Guidelines

Use the **show fabric table** command to display the switch fabric test status. Use the **fabric test** command to test the fabric.

Examples

The following example provides sample output for the **show fabric table** command:

```
[local]RedBack>show fabric table

Fabric status for current timing module (5)
SM/CM   Fabric A   Fabric B   Fabric C   Fabric D
-----   --------   --------   --------   --------
  0      PASSED     PASSED     PASSED     PASSED
  2      PASSED     PASSED     PASSED     PASSED
  3      PASSED     PASSED     PASSED     PASSED
  5      PASSED     PASSED     PASSED     PASSED

SM/CM   Timing 5   Timing 7
-----   --------   --------
  0      PASSED     PASSED
  2      PASSED     PASSED
  3      PASSED     PASSED
  5      PASSED     PASSED
```

The following example provides sample output for the **show fabric table detail** command:

```
[local]RedBack>show fabric table detail

Internal fabric test results for timing module 5
SM/CM   Fabric A   Fabric B   Fabric C   Fabric D
-----   --------   --------   --------   --------
  0      PASSED     PASSED     PASSED     PASSED
  2      PASSED     PASSED     PASSED     PASSED
  3      PASSED     PASSED     PASSED     PASSED
  5      PASSED     PASSED     PASSED     PASSED

External fabric test results for timing module 5
SM/CM   Fabric A   Fabric B   Fabric C   Fabric D
-----   --------   --------   --------   --------
  0      PASSED     PASSED     PASSED     PASSED
  2      PASSED     PASSED     PASSED     PASSED
  3      PASSED     PASSED     PASSED     PASSED
  5      PASSED     PASSED     PASSED     PASSED

Internal fabric test results for timing module 7
SM/CM   Fabric A   Fabric B   Fabric C   Fabric D
-----   --------   --------   --------   --------
  0      PASSED     PASSED     PASSED     PASSED
  2      PASSED     PASSED     PASSED     PASSED
  3      PASSED     PASSED     PASSED     PASSED
  5      PASSED     PASSED     PASSED     PASSED

External fabric test results for timing module 7
SM/CM   Fabric A   Fabric B   Fabric C   Fabric D
-----   --------   --------   --------   --------
  0      PASSED     PASSED     PASSED     PASSED
  2      PASSED     PASSED     PASSED     PASSED
  3      PASSED     PASSED     PASSED     PASSED
  5      PASSED     PASSED     PASSED     PASSED

Fabric status for current timing module (5)
SM/CM   Fabric A   Fabric B   Fabric C   Fabric D
-----   --------   --------   --------   --------
  0      PASSED     PASSED     PASSED     PASSED
  2      PASSED     PASSED     PASSED     PASSED
  3      PASSED     PASSED     PASSED     PASSED
  5      PASSED     PASSED     PASSED     PASSED

SM/CM   Timing 5   Timing 7
-----   --------   --------
  0      PASSED     PASSED
  2      PASSED     PASSED
  3      PASSED     PASSED
  5      PASSED     PASSED
```

Related Commands

fabric test
show fabric counters

show fe stats

show fe stats

Purpose

Displays status information about the Forwarding Engine (FE) module.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show fe stats** command to display the status of the FE module.

Examples

The following example shows sample output from the command:

```
[local]RedBack#show fe stats

--- Global Stats ---
rounds:          3,953,543,431      ticks:               32,411,010
pkts_rcvd:                   0      free_buffers:                 0
buf_alloc_fails:             0      bad_l2_protocol:              0
ce_fepkt_rcvs:               0      ce_fepkt_xmts:                0
bogus_cct_xmts:              0      ce_fepkt_rcv_ring_full:       0
l2_runt_pkts:                0      pppoe_runt_pkts:              0

--- IP Stats ---
ip_pkts_rcvd:                0      ip_pkts_xmtd:                 0
ip_ttl_expired:              0      no_ip_route:                  0
bad_ip_xsums:                0      rcv_bad_ip_ver:               0
arp_resource_errs:           0      no_nxthop_host:               0
arp_decaps_drops:            0      ip_acl_inb_drops:             0
llc_too_small:               0      llc_too_large:                0
ip_acl_outb_drops:           0      ip_cct_acl_inb_drops:         0
```

```
ip_cct_acl_outb_drops:       0       other_ip_errors:              0
invalid_ip_srcs:             0       invalid_ip_dsts:              0
ip_pkts_fragmented:          0       ip_fragments_xmtd:            0
ip_dont_fragment_drops:      0       ip_fragment_runt_pkts:        0
FE reassy's completed:       0       FE mem resource err:          0
FE reassy's canceled:        0       FE reassy buf limit:          0
ip_runt_pkts:                0       not_resolved:                 0
l2_len_<_min_hlen:           0       ip_hlen_too_short:            0
ip_pkt_len_too_short:        0       l2_len_<_ip_len:              0
ip_mcast_pkts_rcvd:          0       ip_mcast_pkts_xmtd:           0
mcast_pkts_fragmented:       0       mcast_fragments_xmtd:         0
l2_mcast_drop:               0

--- L2TP Stats ---
l2tp_pkts_rcvd:              0       l2tp_ce_dlvrs:                0
l2tp_lns_dlvrs:              0       l2tp_lac_dlvrs:               0
l2tp_lns_bypass_dlvrs:       0       l2tp_lac_bypass_dlvrs:        0
l2tp_ip_xmits:               0       l2tp_pvc_xmits:               0
l2tp_ip_errs:                0       last_l2tp_ip_err:             0
l2tp_no_tunnel:              0       l2tp_no_session:              0
l2tp_flow_ctl:               0       l2tp_len_err:                 0
l2tp_no_tid:                 0       l2tp_no_t_bit:                0
l2tp_police_drops:           0       l2tp_rate_drops:              0

--- Bridge Packet Filtering Stats ---
acl_inb_drops:               0       acl_outb_drops:               0
cct_acl_inb_drops:           0       cct_acl_outb_drops:           0
other_acl_inb_errors:        0       other_acl_outb_errors:        0
q8021_no_config:             0
```

Table 42-6 (global statistics), Table 42-7 (IP statistics), Table 42-8 (L2TP statistics), and Table 42-9 (bridge packet filtering statistics) describe of the output fields for the **show fe stats** command:

Table 42-6 Global Stats

Display Field	Description
rounds	Number of times the FE module has cycled through its main loop; indicates how busy the FE is (slower increments indicate that the FE is busier).
ticks	Timing clock for noncritical intervals on the FE module (increments once every 16.67 ms)
pkts_rcvd	Number of packets received by the FE module. Excludes packets from the CE and those packets for which no PVC exists
free_buffers	Not used
buf_alloc_fails	Number of times the FE module has failed when trying to allocate a buffer to send or receive a packet
bad_l2_protocol	Number of packets discarded by the FE module due to an invalid layer 2 protocol header
ce_fepkt_rcvs	Number of data packets transferred from the FE module to the CE module
ce_fepkt_xmts	Number of data packets received by the FE module from the CE module

Table 42-6 Global Stats

Display Field	Description
bogus_cct_xmts	Number of packets transmitted via a port that is no longer configured
ce_fepkt_rcv_ring_full	Number of packets destined to the CE module dropped by the FE module due to congestion between the CE module and FE module
l2_runt_pkts	Number of packets detected as too small while processing layer 2 protocol headers
pppoe_runt_pkts	Number of PPPoE packets with length too small

Table 42-7 IP Stats

Display Field	Description
ip_pkts_rcvd	Number of IP packets received by the FE module
ip_pkts_xmtd	Number of IP packets transmitted by the FE module
ip_ttl_expired	Number of IP packets discarded by the FE module due to expired time-to-live
no_ip_route	Number of IP packets discarded by the FE module because it had no route to the destination
bad_ip_xsums	Number of IP packets discarded by the FE module due to a bad IP checksum
rcv_bad_ip_ver	Number of IP packets discarded by the FE module due to an invalid IP version
arp_resource_errs	Number of IP packets discarded by the FE module due to a lack of resources needed to resolve the destination address
no_nxthop_host	Number of IP packets discarded by the FE module because the next hop was unreachable
arp_decaps_drops	Number of IP packets discarded by the FE module due to an unrecognized encapsulation
ip_acl_inb_drops	Number of IP packets discarded by the FE module due to an inbound IP access list restriction
llc_too_small	Number of IP packets discarded by the FE module due to the packet being too small
llc_too_large	Number of IP packets discarded by the FE module due to the packet size exceeding the frame size
ip_acl_outb_drops	Number of IP packets discarded by the FE module due to an outbound IP access list restriction
ip_cct_acl_inb_drops	Number of IP packets discarded by the FE module due to an inbound circuit-level access list restriction
ip_cct_acl_outb_drops	Number of IP packets discarded by the FE module due to an outbound circuit-level access list restriction
other_ip_errors	Number of IP packets discarded by the FE module due to an unclassified error
invalid_ip_srcs	Number of IP packets discarded by the FE module due to an invalid source address
invalid_ip_dsts	Number of IP packets discarded by the FE module due to an invalid destination address
ip_pkts_fragmented	Number of packets fragmented by the FE module
ip_fragments_xmtd	Number of fragments transmitted by the FE module
ip_dont_fragment_drops	Number of IP packets discarded by the FE module because the packet was flagged as “don’t fragment,” but the packet size exceeded the MTU of the next hop interface.

Table 42-7 IP Stats

Display Field	Description
ip_fragment_runt_pkts	Number of IP packets discarded by the FE module because the receive length was less than the length indicated in the packet
FE reassy's completed	Number of packet reassemblies completed
FE mem resource err	Number of IP packets discarded by the FE module due to a lack of resources needed to reassemble the packet
FE reassy's canceled	Number of IP packets discarded by the FE module due to a delay in receiving all the fragments
FE reassy buf limit	Not used
ip_runt_pkts	Number of IP runts discarded by the FE module
not_resolved	Number of IP packets discarded by the FE module because it could not resolve the destination address
l2_len_<_min_hlen	Number of IP packets discarded by the FE module due to a packet length less than the minimum header length
ip_hlen_too_short	Number of IP packets discarded by the FE module due to an IP header length less than the required minimum for an IP packet
ip_pkt_len_too_short	Number of IP packets discarded by the FE module due to an IP packet length value less than the minimum for an IP packet
l2_len_<_ip_len	Number of IP packets discarded by the FE module due to the frame length being smaller than the IP packet length
ip_mcast_pkts_rcvd	Number of IP multicast packets received by the FE module
ip_mcast_pkts_xmtd	Number of IP multicast packets transmitted by the FE module
mcast_pkts_fragmented	Number of IP multicast packets fragmented by the FE module
mcast_fragments_xmtd	Number of IP multicast fragments transmitted by the FE module
l2_mcast_drop	Number of layer 2 multicast packets dropped by the FE module

Table 42-8 L2TP Stats

Display Field	Description
l2tp_pkts_rcvd	Number of L2TP and L2F data and control packets received
l2tp_ce_dlvrs	Number of L2TP and L2F control packets received
l2tp_lns_dlvrs	Number of L2TP and L2F data packets received at the LNS or HG
l2tp_lac_dlvrs	Number of L2TP and L2F data packets received at the LAC or NAS
l2tp_lns_bypass_dlvrs	Number of L2TP and L2F data packets received at the LNS or HG end of a tunnel switch
l2tp_lac_bypass_dlvrs	Number of L2TP and L2F data packets received at the LAC or NAS end of a tunnel switch
l2tp_ip_xmits	Number of L2TP and L2F data packets transmitted over UDP/IP
l2tp_pvc_xmits	Number of L2TP and L2F data packets forwarded over PVCs
l2tp_ip_errs	Number of transmit failures for L2TP and L2F data packets over UDP/IP

Table 42-8 L2TP Stats

Display Field	Description
last_l2tp_ip_err	Error code corresponding to the last failure to transmit a L2TP/L2F data packet over UDP/IP
l2tp_no_tunnel	Number of L2TP and L2F data packets dropped due to an invalid tunnel ID
l2tp_no_session	Number of L2TP and L2F data packets dropped due to an invalid session ID
l2tp_flow_ctl	Number of L2TP and L2F data packets dropped due to a full session-level window
l2tp_len_err	Number of L2TP and L2F data or control packets dropped due to a length-too-small error
l2tp_no_tid	Number of L2TP and L2F data packets with a zero tunnel ID
l2tp_no_t_bit	Number of L2TP and L2F data packets with a session ID of zero, but not marked as a control packet
l2tp_police_drops	Number of L2TP and L2F data packets dropped due to tunnel-level policing
l2tp_rate_drops	Number of L2TP and L2F data packets dropped due to tunnel-level rate-limiting

Table 42-9 Bridge Packet Filtering Stats

Display Field	Description
acl_inb_drops	Number of packets dropped by the FE module due to an inbound access list restriction.
acl_outb_drops	Number of packets dropped by the FE module due to an outbound access list restriction.
cct_acl_inb_drops	Number of packets dropped by the FE module due to an inbound circuit-level access list restriction.
cct_acl_outb_drops	Number of packets dropped by the FE module due to an outbound circuit-level access list restriction.
other_acl_inb_errors	Number of packets dropped by the FE module due to an unknown error during inbound access list processing.
other_acl_outb_errors	Number of packets dropped by the FE module due to an unknown error during outbound access list processing.
q8021_no_config	Number of packets with 802.1q Ethertype because of no ATM circuit bound to the port via the **bind dot1q** command

Related Commands

show hardware

show hardware

show hardware [**all** | **backplane** | **cm** [*slot*] | **fabric** | **fe** | **midplane** | **power** | *slot*/*port* | **sm** [*slot*] | **timing**]

Purpose

Displays information about the system hardware.

Command Mode

operator exec

Syntax Description

all	Optional. Displays information for all hardware.
backplane	Optional. Displays information about backplane hardware.
cm [*slot*]	Optional. Information about all Connection Manager (CM) modules in the system. When the *slot* argument is used, displays information about the CM module in the specified slot.
fabric	Optional. Displays fabric module information.
fe	Optional. Displays Forwarding Engine (FE) information.
midplane	Optional. Displays midplane hardware information.
power	Optional. Displays power supply information.
slot/*port*	Optional. Slot and port number for a particular port.
sm [*slot*]	Optional. Information about all System Manager (SM) modules in the system. When the *slot* argument is used, displays information about the SM module in the specified slot.
timing	Optional. Displays timing module information.

Default

Displays a summary of all the hardware in the system.

Usage Guidelines

Use the s**how hardware** command to display information about system hardware. To display detailed information about all the hardware in the system, add the **all** keyword. To display detailed information about one specific element, add an optional keyword. Supported keywords vary according to the platform on which the Access Operating System (AOS) is running.

Examples

The following example displays summary information about all hardware in the system on a platform that supports the backplane and FE modules:

```
[local]RedBack>show hardware

Hardware  Ee  Brd  Rwrk Epld Top Feature
Type      Id  Rev  Rev  Rev  Rev Bits  Serial Number    Part Number     Phy Type
-----     --  ---  ---  ---  --- ----  -------------    -----------     --------
BACKPLANE  2  0.1  0.1  0.1  0.1 0000  12345678901234   12345678901234
AC POWER   2  0.1  0.1  0.1  0.1 0000  12345678901234   12345678901234
FE         2  0.1  0.1  0.4  0.5 0000  12345678901234   12345678901234
ENET (3/0) 2  0.1  0.1  0.1  0.1 0000  12345678901234   12345678901234  100TX
ENET (3/1) 2  0.1  0.1  0.1  0.1 0000  12345678901234   12345678901234  100TX
TE   (4/0) 2  0.3  0.*  0.*  0.A 0000  940A1060066271   600-0139-0A
TE   (4/1) 2  0.3  0.*  0.*  0.A 0000  940A1060066271   600-0139-0A
ATDS3(6/0) 2  0.1  0.1  0.1  0.1 0000  12345678901234   12345678901234  BNC
ATDS3(6/1) 2  0.1  0.1  0.1  0.1 0000  12345678901234   12345678901234  BNC
```

The following example provides additional detail about port `3/0`:

```
[local]RedBack>show hardware 3/0

   slot (3/0)              id_version:     2
   hardware type:   ENET   vendor:         RedBack
   board revision:  0.1    serial number:  051019810118
   rework revision: 0.1    part number:    600-0106-01
   epld revision:   0.1    feature_bits:   0
   assembly rev:    0.1    checksum:       4b7b
   No. Mac Addrs:   1      Mac Address:    00:10:67:00:10:6c
   Physical connector: 100TX
```

The following example provides additional detail about port `4/0`:

```
   [local]RedBack>show hardware 4/0

   slot (4/0)              id_version:     2
   hardware type:  TE      vendor:         Redback
   board revision: 0.3     serial number:  940A1060066271
   rework revision:0.*     part number:    600-0139-0A
   epld revision:  0.*     feature_bits:   0
   assembly rev:   0.A     checksum:       3da1
   No. Mac Addrs:  0       Mac Address:    00:00:00:00:00:00
   Physical connector:
```

The following example displays summary information about all hardware in the system on a platform that supports the midplane and timing, fabric, CM, and SM modules:

```
[local]RedBack>show hardware

HW       Slot/  Ee  Brd  Rwrk Pld Top   Feature                          Phy Type
Type     Port   Id  Rev  Rev  Rev  Rev   Bits    Serial Number  Part Number  Or Memory
-------  ------ --  ---  ---  ---  ---   ---- -------------  -----------  -----
MIDPLANE        3   0.1  0.1  0.1  0.5   0000    xx011030000001 600-0151-01
FABRIC   a      3   0.1  0.1  0.1  0.1   0000    68011030000001 600-0150-01
FABRIC   b      3   0.1  0.1  0.1  0.1   0000    68011030000002 600-0150-01
FABRIC   c      3   0.1  0.1  0.1  0.1   0000    68011030000003 600-0150-01
FABRIC   d      3   0.1  0.1  0.1  0.1   0000    68011030000004 600-0150-01
TIMING   5      2   0.1  0.1  0.1  0.1   0000    70011030000001 600-0153-01
TIMING   7      2   0.1  0.1  0.1  0.1   0000    70011030000002 600-0153-01
CM       0      2   0.1  0.0  0.0  0.1   0000    91011030000001 600-0149-01   512MB
 POSOC12   1/0  2   0.1  0.1  0.1  0.1   0000    74011030000001 600-0164-01   SM
 POSOC12   1/1  2   0.1  0.1  0.1  0.1   0000    74011030000002 600-0164-01   SM
CM       1      2   0.1  0.0  0.0  0.1   0000    91011030000002 600-0149-01   512MB
 POSOC12   3/0  2   0.1  0.1  0.1  0.1   0000    74011030000003 600-0164-01   SM
 POSOC12   3/1  2   0.1  0.1  0.1  0.1   0000    74011030000004 600-0164-01   SM
SM       2      3   0.1  0.1  0.1  0.1   0000    67011030000001 600-0148-01   512MB
 ENET      4/0  2   0.1  0.1  0.1  0.1   0000    69011030000001 600-0226-01   100TX
SM       3      3   0.1  0.1  0.1  0.1   0000    67011030000002 600-0148-01   512MB
 ENET      6/0  2   0.1  0.1  0.1  0.1   0000    69011030000002 600-0226-01   100TX
CM       4      2   0.1  0.0  0.0  0.1   0000    91011030000003 600-0149-01   512MB
 AT2OC3    8/0  2   0.1  0.1  0.1  0.1   0000    80011030000001 600-0176-01   SM
 AT2OC3    8/1  2   0.1  0.1  0.1  0.1   0000    80011030000002 600-0176-01   SM
 AT2DS3    9/0  2   0.1  0.1  0.1  0.1   0000    81011030000001 600-0178-01   BNC
 AT2DS3    9/1  2   0.1  0.1  0.1  0.1   0000    81011030000002 600-0178-01   BNC
CM       5      2   0.1  0.0  0.0  0.1   0000    91011030000004 600-0149-01   512MB
 AT2OC3   10/0  2   0.1  0.1  0.1  0.1   0000    80011030000003 600-0176-01   SM
 AT2OC3   10/1  2   0.1  0.1  0.1  0.1   0000    80011030000004 600-0176-01   SM
 AT2DS3   11/0  2   0.1  0.1  0.1  0.1   0000    81011030000003 600-0178-01   BNC
 AT2DS3   11/1  2   0.1  0.1  0.1  0.1   0000    81011030000004 600-0178-01   BNC

CM      11      2   0.1  0.0  0.0  0.1   0000    91011030000002 600-0149-01   512MB
 GBENET   23/0  2   0.1  0.1  0.1  0.1   0000    71011030000001 600-0224-01   1000LX
 GBENET   23/1  2   0.1  0.1  0.1  0.1   0000    71011030000002 600-0224-01   1000LX
```

The following example provides additional detail about the SM module in slot 2:

```
[local]RedBack>show hardware sm 2

SM2                       id_version:     1
hardware type:  SM        vendor:         RedBack
board revision: 0.1       serial number:  67011030000001
rework revision:0.1       part number:    600-0148-01
prog load rev:  0.1       feature_bits:   0
assembly rev:   0.1       checksum:       9a46
no. MAC addrs:  1         MAC address:    00:10:67:00:58:be
memory size: 512 megabytes
```

The following example provides additional detail about the I/O module in slot 23 on port 0:

```
[local]RedBack>show hardware 23/0

slot (23/0)             id_version:     1
hardware type: GBENET   vendor:         RedBack
board revision: 0.1     serial number:  69011030000001
rework revision:0.1     part number:    600-0224-01
prog load rev:  0.1     feature_bits:   0
assembly rev:   0.1     checksum:       9a46
no. MAC addrs:  1       MAC address:    00:10:67:00:58:be
physical connector: 1000LX
```

Related Commands

show port info

show ip socket

show ip socket

Purpose

Displays a table of all Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP) sockets in use in the current context.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show ip socket** command to view the TCP and UDP sockets in use in the current context.

Examples

The following example shows sample output from the **show ip socket** command:

```
[local]RedBack>show ip socket

Active Internet connections (including servers)
PCB     Proto Recv-Q Send-Q Local Address Foreign Address state)
------- ----- ------ ------ ------------- -------------- ----------
1db73d0 TCP    0     205    10.1.1.1.23   10.1.1.2.1339   ESTABLISHED
1db76d0 TCP    0     0      0.0.0.0.23    0.0.0.0.0       LISTEN
1db7650 UDP    0     0      0.0.0.0.520   0.0.0.0.0
1db7750 UDP    0     0      0.0.0.0.1812  0.0.0.0.0
```

Related Commands

show process
show ip traffic

show ip traffic

show ip traffic [**arp** | **general** | **icmp** | **igmp** | **tcp** | **udp**]

Purpose

Displays IP packet statistics for the current context.

Command Mode

operator exec

Syntax Description

arp	Optional. Display only a summary of ARP statistics.
general	Optional. Display only a summary of general IP statistics.
icmp	Optional. Display only a summary of Internet Control Message Protocol (ICMP) statistics.
igmp	Optional. Display only a summary of Internet Group Management Protocol (IGMP) statistics.
tcp	Optional. Display only a summary of Transmission Control Protocol (TCP) statistics.
udp	Optional. Display only a summary of Universal Datagram Protocol (UDP) statistics.

Default

Displays a summary of traffic statistics for all IP protocols.

Usage Guidelines

Use the **show ip traffic** command to display IP packet statistics for the current context. IP traffic statistics are gathered for traffic destined to the system itself and do not include forwarded traffic.

Examples

The following example displays all UDP traffic destined to, or sourced by the system:

```
[local]RedBack>show ip traffic udp

UDP statistics:
     Rcvd: 534 total, 0 bad format
           0 checksum errors, 521 no port
           0 full socket 1 pcb lookup failure
     Sent: 12 total
```

Related Commands

show port counters

show memory

show memory [**ce** | **cm** *slot* | **fe** | **sm** | **te**]

Purpose

Displays system memory statistics.

Command Mode

operator exec

Syntax Description

ce	Optional. Displays Control Engine (CE) module memory usage.
cm *slot*	Optional. Displays Connection Manager (CM) module memory usage. The slot number of the CM must be specified.
fe	Optional. Displays Forwarding Engine (FE) module memory usage.
sm	Optional. Displays the System Manager (SM) module memory usage.
te	Optional. Displays the Transform Engine (TE) module memory usage. The IP Security (IPSec) module has two TE ports.

Default

Displays summary memory usage information.

Usage Guidelines

Use the **show memory** command to display statistics about the available and allocated memory in the system memory partition. It is useful for determining if the system is running low on available memory.

Examples

The following example shows sample output from the **show memory** command:

```
[local]RedBack>show memory

FRI MAR 05 09:56:55 1999
     Free Bytes   Bytes in Use  Blocks In Use  Cumul. Blocks
     ----------   ------------  -------------  -------------
CM   19,406,372     6,407,284           1,445          6,469
SM     2,933,120         904,832              104             104
```

The following example shows output from the **show memory** command when the **te** keyword is specified. The IPSec/Compression Transform Engine (TE) has two ports. This output displays memory usage for both ports:

```
[local]popeye>show memory te

THU APR 02 22:18:22 2043
TE port: 4/0
   Free Bytes Bytes in Use Blocks In Use Cumul. Blocks
   ---------- ------------ ------------- -------------
TE 1,223,680  873,472      2,540         4,787

TE port: 4/1
   Free Bytes Bytes in Use Blocks In Use Cumul. Blocks
   ---------- ------------ ------------- -------------
TE 1,364,992  732,160      2,407         4,652
```

Related Commands

buffers—port configuration mode
buffers—Frame Relay profile configuration mode

show process

show process [**cpu** [**non-zero**]]

Purpose

Displays a synopsis of the processes in the system.

Command Mode

operator exec

Syntax Description

cpu	Optional. Display average CPU utilization statistics for five-second, one-minute, and five-minute intervals for processes.
non-zero	Optional. Display only processes with nonzero CPU utilization values.

Default

Displays a synopsis of all processes in the system.

Usage Guidelines

Use the **show process** command to display a synopsis of the processes in the system. This command is intended to be used only as a debugging aid because the information is obsolete by the time it is displayed.

Examples

The following example shows sample output from the **show process** command:

```
[local]RedBack>show process

WED JUN 09 10:10:11 1999
  NAME         ENTRY    TID     PRI  STATUS    PC      SP       ERRNO    DELAY
------------   -------  ------- ---  --------- ------- -------- -------- -----
tExcTask       3f1e40   1e43f40   0  PEND      40a52d  1e43eb0  3d0001     0
tLogTask       3f3ba4   1e3c388   0  PEND      40a52d  1e3c2f4       0     0
Dr_K           2a8bd0   1dbc7d0   0  SUSPEND   3e1c26  1dbc794       0     0
tWatchWarn     2ad434   1e12800   1  PEND      40a52d  1e12754       0     0
tIsr           2aac98   1d907d0   1  PEND      3dc55d  1d90794       0     0
tNmi           2ab6ec   1d327d0   1  PEND      40a52d  1d32558       0     0
tPcmciad       3d336c   1d8af40   2  PEND      40a52d  1d8aeb0       0     0
tTelnetd       20d108   1a66388   2  PEND      3dc55d  1a662a8       0     0
```

```
tTnetOut0      20d638   1a4a388   2  PEND      3dc55d  1a4a0e8       0     0
tTnetIn0       20d6e8   1a32388   2  PEND      3dc55d  1a3204c       0     0
tTnetOut2      20d638   19a8388   2  PEND      3dc55d  19a80e8       0     0
tTnetIn2       20d6e8   19a1388   2  PEND      3dc55d  19a104c       0     0
tTnetOut1      20d638   19d2388   2  PEND      3dc55d  19d2060       0     0
tTnetIn1       20d6e8   19cc388   2  PEND      3dc55d  19cc04c       0     0
tWdbTask       405d24   1e35000   3  PEND      3dc55d  1e34f54       0     0
tDetect        2a832c   1d377d0  50  PEND      3dc55d  1d37774       0     0
tEnvMon        183040   1d2c7d0  50  DELAY     3e2236  1d2c76c       0   179
tPeriodic      2ad750   1c497d0  50  DELAY     3e2236  1c4978c       0   179
ppp_auth       296efc   1be7000  50  PEND      3dc55d  1be6f7c    3006b    0
t21140fatal    115420   1ab6800  50  PEND      3dc55d  1ab67c0       0     0
```

The following example includes CPU usage statistics, and only displays processes with non-zero counters:

```
[local]RedBack>show process cpu non-zero

WED JUN 09 10:47:57 1999
CPU Utilization for 5 seconds: 2%    1 Minute: 5%    5 Minutes: 1%

NAME          PRI   TIME (ms)    CALLS      5Sec    1Min    5Min    LONGEST(ms)
------------  ---   ---------    -----      ----    ----    ----    ----
t21140tx       50   46,746       3,720      0%      2%      0%      16
ip_rx         150   236,063      34,910     1%      2%      1%      16
tFEPkt        254   154,829,288  9,394,301  97%     94%     98%     16
```

Related Commands

show memory

show slot

show slot {**table** | *slot*}

Purpose

Displays information about the I/O module information.

Command Mode

operator exec

Syntax Description

table	Displays the entire slot table.
slot	Specific slot number to be displayed. The range of values is 0 to 32.

Default

None

Usage Guidelines

Use the **show slot** command to display I/O module information.

Examples

The following example shows sample output from the **show slot table** command:

```
[local]RedBack>show slot table

I/O Slot Table contents are:

Slot 0 type is DEC 21140.
Slot 4 type is Brooktree 8233.
```

Related Commands

show port info
show port table

show sram

show sram

Purpose

Displays the amount of static random access memory (SRAM) and the format of data stored for each PCMCIA card.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show sram** command to displays the amount of SRAM and the format of data stored for each PCMCIA card. The data format can be either file system (for example, DOS) or Dynamic Host Control Protocol (DHCP) secured-Address Resolution Protocol (ARP).

Examples

The following example displays information when the device is formatted with a file system:

```
[local]RedBack>show sram

Device /pcmia0 is a 6291456 byte SRAM card, formatted with a DOS File
System
```

The following example displays when the device is formatted for DHCP secured-ARP:

```
[local]RedBack>show sram

Device /pcmia0 is a 6291456 byte SRAM card, formatted for
dhcp-secured-arp
```

Related Commands

dhcp preserve-state
format

show stack

show stack

Purpose

Displays information about the last system restart.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show stack** command to display the saved stack information from a restart caused by a system error. If an exception resulting in a reload occurs, a complete traceback is automatically saved to the inactive log upon reload.

Examples

The following examples show sample output from the **show stack** command:

```
[local]RedBack>show stack

   System restarted normally by reload, no stack available.

[local]RedBack>show stack

   System restarted by exception 14 while running version 1.0.1.13.

   Stack trace: 0x10ca06 0x10c9d1 0x10c9ac 0x10c987 0x10c963
```

Related Commands

show log
show version

show subscribers

show subscribers [**access-statistics** [*sub-name*] | **active** [*sub-name*] | **address** *sub-name* | **all** | **minimums** [*ctx-name* | **all**] | **summary**]

Purpose

Displays subscriber information.

Command Mode

operator exec

Syntax Description

access-statistics *sub-name*	Optional. Displays the number of incoming and outgoing packets filtered by the access control list. If *sub-name* is not specified, access statistics are displayed for all subscribers in the context. If *sub-name* is used, only access statistics for that subscriber are displayed.
active *sub-name*	Optional. List of active users.
address *sub-name*	Optional. IP addresses currently in use by the specified subscriber.
all	Optional. Displays information for subscribers in all contexts. This option is available only to operators and administrators in the local context.
minimums *ctx-name* | **all**	Optional. When the *ctx-name* argument is not specified, displays reserved subscriber slots for the current context. When the *ctx-name* argument is specified, displays reserved subscriber slots for that context. When the **all** keyword is specified, reserved subscriber slots for all contexts are displayed. The **all** keyword is available only when the current context is local.
summary	Optional. Displays a summary of subscriber information.

Default

Displays information for all active subscribers in the current context.

Usage Guidelines

Use the **show subscribers** command to display subscriber information.

You must specify the **access-statistics** keyword in the context in which the subscriber whose information is being queried is configured.

When you use the **address** keyword, nothing is displayed if the subscriber is currently not logged on or has no IP addresses. This command will display all addresses for RFC 1483-encapsulated or RFC 1490-encapsulated subscriber circuits and for Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE) subscribers. It displays Dynamic Host Configuration Protocol (DHCP)-assigned addresses and authentication, authorization, and accounting (AAA)-assigned addresses.

Use the **minimums** keyword to display, at the context and tunnel peer level, the minimum number of subscriber slots reserved in the current context. If the current context is local, you have the additional options of displaying reserved minimums for a specific context other than local or for all contexts. Reserved subscriber minimums are set using either the **aaa min-subscribers** command (context level reservation) or the **l2x profile** and **profile** commands (tunnel peer level reservation).

The **summary** keyword omits per-subscriber information and prints only the total number of subscribers and their encapsulations. A subscriber name appears in the table whenever the corresponding link is up.

Note This command is also described in Chapter 42, "System Monitoring and Testing Commands."

Examples

The following example demonstrates the default information provided by the **show subscribers** command:

```
[local]RedBack>show subscribers

 CIRCUIT       SUBSCRIBER         CONTEXT     START TIME
 ------------------------------------------------------------------
 PPPOE 00001   pppoe@redback.com  redback.com FRI DEC 04 17:46:49 1998
 ------------------------------------------------------------------
 Total = 1 (ppp = 1, r-1483 = 0, b-1483 = 0, r-1490 = 0, b-1490 = 0)

[local]RedBack>show subscribers address pppoe

Host            Nhop cct    Interface
155.53.196.2    7000001     pool
```

The example below demonstrates the use of the **access-statistics** keyword:

```
[local]RedBack>show subscribers access-statistics

Subscriber name: atm501@local
Inbound IP access-statistics:
permit = 0 deny = 0
redir = 0 bad redir = 0
```

The following example shows using the **show subscribers minimums** command in the local context to display reserved subscriber minimums in all contexts.

Note When the word `implied` appears in parentheses in the output, it means that the subscriber slots are reserved at the tunnel peer level as opposed to being reserved at the context level. The reservation at the context level is, therefore, implied.

```
[local]RedBack>show subscriber minimums all

Total subscribers in the system: 4000

CONTEXT      TUNNEL    MIN. SUB(Context)  MIN. SUB(Tunnel)  OCCUPIED
=====================================================================
             gentle                       200               0
local                  200 (Implied)
---------------------------------------------------------------------
              ben                         10                0
tribune                 10 (Implied)
---------------------------------------------------------------------
Total                  210                                  0

Unreserved slots: 3790
Currently occupied unreserved slots: 0
```

The following example shows using the **show subscribers minimums** command in the local context to display reserved subscriber minimums for the context called `tribune`:

```
[local]RedBack>show subscriber minimums tribune

Minimum Subscribers (Implied):  10

TUNNEL PROFILE        MIN. SUBSCRIBERS        OCCUPIED
=======================================================
ben                   10                      0
```

Related Commands

aaa min-subscribers
bridge-group
clear circuit
clear subscriber
interface
ip access-group—subscriber configuration mode
ip address—subscriber configuration mode
show bindings
show ppp
subscriber

show tech

show tech *url* [**compress-level** *level*] [**details**] [**-noconfirm**] [**show-password**]

Purpose

Saves information about the state of the system into a technical support file.

Command Mode

administrative exec

Syntax Description

url	Name of the technical support file including the device and optional subdirectory where the file is to be located.
compress-level *level*	Compression level of the technical support file. The range of values is 0 to 9; the default is 6.
details	Specifies that feature-specific information is to be included in the display.
-noconfirm	Specifies that the existing technical support file is to be replaced without asking for confirmation.
show-password	Specifies that the display is to include passwords, rather than masking the passwords.

Default

None

Usage Guidelines

Use the **show tech** command to save system information to a file. This command is designed to compile information about the system that can be used by technical support personnel for troubleshooting purposes.

When supplying a directory path using the *url* argument, you must use the following form:

/device[/*path*]/*filename*

The */device* argument can be **/flash**, **/pcmcia0**, or **/pcmcia1** (depending on your hardware platform). The /*path* argument is an optional subdirectory. The /*filename* argument is the name of the technical support file.

Use the **compress-level** *level* construct to specify how compressed you want the resulting file to be. The higher the value of the *level* argument, the more compressed the file. A compression level of 0 creates a file that is not compressed at all.

Use the **directory** command to verify that the file was created as intended, and to display the size of the file.

Examples

The following example creates an uncompressed (compression level `0`) file called `tech.z` on the `/pcmcia0` device. If a `tech.z` file already exists on this device, the system is to overwrite it without asking the administrator for confirmation:

```
[local]RedBack#sh tech /pcmcia0/tech.z compress-level 0 -noconfirm

!!!!!!!!!!!!!!!!!
Original data size: 101858
Size of compressed data: 101878
Compression ratio: 1:1.00
MD5 checksum of uncompressed data: 173c333ed1367fb7d975638bdd526e37
```

The following example shows using the **directory** command to display statistics about the resulting file:

```
[local]RedBack#dir /pcmcia0/tech.z

SM3 (Active):
-------------
  size       date            time       name
  -------    ------          ------     -------
  102618     JUN-07-2001     15:34:44   /pcmcia0/tech.z
```

Related Commands

directory
show hardware

traceroute

traceroute {*ip-address* | *hostname*} [**count** *number*] [**df**] [**maxttl** *ttl*] [**minttl** *ttl*] [**port** *port*] [**size** *bytes*] [**src** *ip-address*] [**timeout** *seconds*]

Purpose

Traces the IP route to a destination.

Command Mode

operator exec

Syntax Description

hostname	Hostname to be traced. Domain Name Service (DNS) must be enabled.
ip-address	IP address to be traced.
count *number*	Optional. Number of probes to send.The range of values is 1 to 1,000; the default is 3.
df	Optional. Sets the “Don’t Fragment” bit on outbound traceroute packets. With this bit set, the traceroute packet is dropped whenever it would normally be fragmented. An Internet Control Message Protocol (ICMP) “Unreachable, Needs Fragmentation” packet is sent to the sender.
maxttl *ttl*	Optional. Maximum time to live. The range of values is 1 to 255; the default is 30.
minttl *ttl*	Optional. Minimum time to live. The range of values is 1 to 255; the default is 1.
port *port*	Optional. Destination Universal Datagram Protocol (UDP) port number. The range of values is 1 to 65,535; the default is 33,434.
size *bytes*	Optional. The datagram size in octets. The range of values is 40 to 2,000; the default is 140.
src *ip-address*	Optional. IP source address of the ping packets. An interface with this IP address must exist.
timeout *seconds*	Optional. Amount of time, in seconds, for each probe sent. The range of values is 1 to 1,000; the default is 2.

Default

The **traceroute** command sends three 140-byte packets on UDP port 33434, using a timeout of 2 seconds and a time to live value of 30.

Usage Guidelines

Use the **traceroute** command to discover the routes that packets will take when travelling to the specified destination. Each line in the display shows the next hop in the path between the system and the destination address.

The *hostname* option can only be used if DNS is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands in context configuration mode. See Chapter 28, "DNS Commands."

Press **Ctrl+C** to stop a traceroute.

The **ping** and **traceroute** commands can have vastly different outcomes, depending on the context in which the commands are executed. In particular, a destination (as denoted by an IP address) that can be reached by the **ping** or **traceroute** command in one context might not be reachable from another context.

Examples

The following command discovers the route from the local context to the IP address `206.124.29.1`, using `100`-byte packets, UDP `port 73`, `ttl 20`, `timeout 3` and `count 3`:

```
[local]RedBack>traceroute 206.124.29.1 timeout 3 count 3 ttl 20 port 73 size 100

  traceroute to (206.124.29.1), 20 hops max, 140 byte packets
   1  155.53.145.254 (155.53.145.254)  0 ms  0 ms  0 ms
   2  155.53.200.254 (155.53.200.254)  0 ms  0 ms  16 ms
   3  206.83.66.193 (206.83.66.193)  16 ms  16 ms  16 ms
   4  206.83.90.66 (206.83.90.66)  16 ms  16 ms  16 ms
   5  157.130.193.197 (157.130.193.197)  16 ms  33 ms  16 ms
   6  157.130.194.18 (157.130.194.18)  16 ms  33 ms  16 ms
   7  209.104.192.49 (209.104.192.49)  50 ms  66 ms  50 ms
   8  209.104.198.38 (209.104.198.38)  50 ms  66 ms  66 ms
   9  206.124.1.22 (206.124.1.22)  66 ms  66 ms  66 ms
  10  206.124.29.1 (206.124.29.1)  83 ms  66 ms  83 ms
```

Related Commands

ip domain-lookup
ip domain-name
ip name-servers
ping

Bulk Statistics Commands

This chapter describes the commands used to configure and maintain bulk statistics (bulkstats) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure and maintain bulkstats, and configuration examples, see the “Configuring Bulk Statistics” chapter in the *Access Operating System (AOS) Configuration Guide*.

bulkstats collection

bulkstats collection

no bulkstats collection

Purpose

Enables the collection of system statistics.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

Bulk statistics are not collected by default.

Usage Guidelines

Use the **bulkstats collection** command enable the collection of system statistics. Before you enable bulkstats collection, you must configure:

- One or more schema, using the **bulkstats schema**, **schema,** or **schema profile** command.
- The primary receiver, using the **receiver** command.
- The directory where samples and collection files are stored, using the **localdir** command.
- The name and location of the collection files on the server, using the **remotefile** command.

Use the **no** form of this command to disable bulkstats collection.

Examples

The following command enables the collection of bulk statistics:

```
[local]RedBack(config)#bulkstats collection
```

Related Commands

bulkstats schema
localdir
receiver
remotefile
schema
schema profile
show bulkstats

bulkstats force transfer

bulkstats force transfer

Purpose

Transfers system statistics data to one of the configured receivers.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

Bulkstats data is transferred at scheduled intervals.

Usage Guidelines

Use the **bulkstats force transfer** command to immediately transfer the bulkstats file to a configured receiver, rather than waiting for the next transfer interval. Data is transferred to the primary receiver; if this transfer should fail, data is transferred to the secondary receiver.

Use the **transfer-interval** command in bulkstats configuration mode to modify the interval at which the Access Operating System (AOS) transfers data files to the configured receiver.

Examples

The following example shows how to force the bulkstats file to be transferred immediately to one of the configured receivers:

```
[local]RedBack>bulkstats force transfer
```

Related Commands

transfer-interval

bulkstats mode

bulkstats mode

Purpose

Enters bulkstats configuration mode.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **bulkstats mode** command to enter bulkstats configuration mode.

Examples

The following command enters bulkstats configuration mode:

```
[local]RedBack(config)#bulkstats mode
[local]RedBack(config-bulkstats)#
```

Related Commands

bulkstats collection

bulkstats schema

bulkstats schema *name* {**format** *format-string* | **profile** *profile-name*}
[*AOS-variable* [*AOS-variable...*]]

no bulkstats schema *name*

Purpose

Defines the schema for the contents of the bulkstats collection file for Asynchronous Transfer Mode (ATM) profiles, context profiles, Frame Relay profiles, High-Level Data Link Control (HDLC) channels, the default Layer 2 Tunneling Protocol (L2TP) peer, ports, and the default subscriber.

Command Mode

ATM profile configuration
context configuration
Frame Relay profile configuration
HDLC channel
L2TP peer configuration
port configuration
subscriber configuration

Syntax Description

name	Name of the schema. Can be no more than 19 characters in length.
format *format-string*	Format string that can contain anything or nothing as a label for an AOS variable. The string is used to format the output of the schema. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. Table 43-1 describes the special-character sequences.
profile *profile-name*	Name of the bulkstats schema profile to be applied to multiple ports. Port configuration mode only. See the **schema profile** global configuration mode command.
AOS-variable	Optional. AOS variable for which data is collected. A variable replaces its associated *format-string* definition. Separate the variables with a space. Table 43-2 lists all variables. Supported variables vary according to configuration mode.

The special-character sequences described in Table 43-1 are supported:

Table 43-1 Format String Special-Character Sequences

Syntax	Description
\n	Creates a new line
%s	A character string
%d	An integer in decimal (base 10)
%u	An unsigned integer in decimal (base 10)
%x	An integer in hexadecimal format (base 16)
%%	Gets replaced by a single % character in the output

Table 43-2 AOS Variables Used with bulkstats schema Command

.

AOS Variable	Type	Configuration Mode	Description
active_sessions	Integer	L2TP peer	Active L2TP sessions for the context
activessubs	Integer	context	Active subscribers for the context
active_tunnels	Integer	L2TP peer	Active L2TP tunnels for the context
bind_type	String	subscriber	Subscriber bind type
cct_handle	Integer	subscriber	Subscriber circuit
cctstate	String	ATM profile Frame Relay profile	Circuit status
channel	Integer	Frame Relay profile	Channel on the channelized DS-3 card
context_name	String	context subscriber	Name of the context
description	String	ATM profile Frame Relay profile HDLC channel L2TP peer port	Descriptive text
dlci	Integer	Frame Relay profile	Data-link circuit identifier
epochtime	Integer	all	Time of day in epoch format (seconds since 1/1/1970)
inoctets	Integer	all	Number of octets received on this circuit
inpackets	Integer	all	Number of packets received on this circuit
ip_addr	String	subscriber	Subscriber IP address
ip_mask	String	subscriber	Subscriber netmask

AOS Variable	Type	Configuration Mode	Description
mcast_inoctets	Integer	ATM profile Frame Relay profile port subscriber	Number of multicast octets received on this circuit
mcast_inpackets	Integer	ATM profile Frame Relay profile port subscriber	Number of multicast packets received on this circuit
mcast_outoctets	Integer	ATM profile Frame Relay profile port subscriber	Number of multicast octets sent on this circuit
mcast_outpackets	Integer	ATM profile Frame Relay profile port subscriber	Number of multicast packets sent on this circuit
outoctets	Integer	all	Number of octets sent from this circuit
outpackets	Integer	all	Number of packets sent on this circuit
peer_name	String	L2TP peer configuration	Name of the L2TP peer
port	Integer	ATM profile Frame Relay profile HDLC channel port	Port number on the I/O module
portspeed	String	port	Port speed in kbps
porttype	String	port	Port type
rcv_dropped	Integer	port	Receive packets dropped
slot	Integer	ATM profile Frame Relay profile HDLC channel port	Slot number in the SMS device
subscriber_name	String	subscriber	Name of the subscriber
sysuptime	Integer	all	System uptime in seconds
vpi	Integer	ATM profile	Virtual path identifier
vci	Integer	ATM profile	Virtual circuit identifier
xmt_dropped	Integer	ATM profile Frame Relay profile port	Transmit packets dropped
xmt_outstanding	Integer	ATM profile Frame Relay profile port	Transmit packets outstanding

Default

None

Usage Guidelines

Use the **bulkstats schema** command to define the schema for the contents of the bulkstats collection file. A single bulkstats schema is allowed per context. In subscriber configuration mode, a bulkstats schema can only be applied to a default subscriber. You can only configure one bulkstats schema for the default subscriber. The default subscriber configuration applies to all subscribers within the context. Changes to the bulkstats schema will be applied to subscribers when new sessions are started. In L2TP configuration mode, you can only apply the bulkstats schema to the default L2TP peer.

Caution It is possible to configure multiple schemas, each gathering a different type and format of data. It is advisable to minimize the number of schemas used in order to reduce impact on system performance. This is especially true for ATM profile, Frame Relay profile, HDLC channel, and port schemas. In those modes, you can instead create one schema that will record several subsets of data. Separate each subset within the format string by entering \n to create a new starting line in the output file.

Use the **no** form of this command to delete the specified bulkstats schema.

Examples

The following example creates a schema named `sample`:

```
[local]RedBack(config-port)#bulkstats schema sample format "port: %u, slot: %u,
inpackets: %u, outpackets: %u, description: %s \n" port slot inpackets outpackets
description
```

The result of the previous schema is formatted as follows:

```
sample: port:0, slot:8, inpackts:358145616, outpackets:1010195698,
description: This is dragon-ds3-port 8/0!
```

Related Commands

schema
schema-dump
schema profile

header format

header format *format-string* [*AOS-variable* [*AOS-variable* ...]]

no header format

Purpose

Configures lines of informative text that are inserted at the beginning of the bulkstats collection file.

Command Mode

bulkstats configuration

Syntax Description

format-string String used to format the filename. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks.

The following special-character sequences are supported:

\n—Creates a new line

%s—A character string

%d—An integer in decimal (base 10)

%u—An unsigned integer in decimal (base 10)

%x—An integer in hexadecimal format (base 16)

%%—Gets replaced by a single % character in the output

AOS variable Optional. Access Operating System (AOS) system variable. The following variables can be used:

date—Today's date in YYYYMMDD format (string)

epochtime—Time of day in epoch format (seconds since January 1, 1970); string

hostname— Hostname as specified in the configuration file (string)

sysuptime— System uptime in seconds (integer)

timeofday—Time of day in HHMMSS format (using a 24-hour clock) (string)

Default

None

Usage Guidelines

Use the **header format** command to insert lines of informative text at the beginning of the collection file. Lines added by using this command are inserted in the file in the order in which they are configured.

Each header definition must be unique. If a new header line is configured so that it exactly matches an existing header line, the new header is ignored.

Use the **no** form of this command to delete all bulkstats header specifications in the bulkstats file. After this command is used, all headers must be redefined. Use a text editor for minor editing of the headers rather than editing through system configuration commands.

Example

The following example inserts a line of text in the collection file about the date that data is collected.

```
[local]RedBack(config-bulkstats)#header format "Data collected on %s" date
```

The previous line puts the following line in the collection file:

```
Data collected on 19990315
```

Related Commands

bulkstats collection

limit

limit *kilobytes*

default limit

Purpose

Sets a limit on the space used to store bulkstats data.

Command Mode

bulkstats configuration

Syntax Description

kilobytes	Amount of space (KB) used to store bulkstats data. The range of values is 0 to 4,294,967,295. A value of 0 indicates no limit. The default value is 1,024.

Default

The limit for storing bulkstats data is 1,024 KB (or 1 MB).

Usage Guidelines

Use the **limit** command to set a limit on the space used to store bulkstats data. Changing the limit size while bulkstats collection is enabled disables bulkstats collection. You must re-enable bulkstats collection. If bulkstats collection is re-enabled after a new value has been set, data is deleted, and a new collection file is created.

It is best to use a nonzero value as the limit. Using 0 as the limit value allows the file to grow until the file system is filled. Once the file system is full, the latest data collected is lost because writing to the file will fail until the file is transferred and deleted. When the limit is set to a nonzero value, if data collection fails or if the file size reaches the limit before collection, the oldest data is overwritten, which allows collection to continue with the most recent data saved.

Use the **default** form of this command to return the bulkstats data storage limit to 1,024 KB.

Examples

The following example limits the space used to store bulkstats data to `4906` KB:

```
[local]RedBack(config-bulkstats)#limit 4906
```

Related Commands

localdir

localdir

localdir *dir-name*

no localdir *dir-name*

Purpose

Identifies the local directory where bulkstats samples and collection files are stored on the Subscriber Management System (SMS) device.

Command Mode

bulkstats configuration

Syntax Description

dir-name	Local directory where samples and collection files are stored.

Default

None

Usage Guidelines

Use the **localdir** command to specify the local directory where bulkstats samples and collection files are stored. You must first create a local directory using the **mkdir** command in administrative exec mode before enabling bulkstats collection. You can specify a directory on /pcmcia*x* or /flash (pcmcia*x* is preferrable due to faster write speed). You can limit the space allowed for bulkstats storage with the **limit** command.

If you use the **localdir** command to change the storage directory, you must re-enable collection by using the **bulkstats collection** command in global configuration mode.

Use the **no** form of this command to remove the configuration of the current local directory used to store bulkstats data. You should disable bulkstats collection before changing the local directory.

Example

The following example stores bulkstats collection files in the `pcmcia0/blksts` directory:

```
[local]RedBack(config-bulkstats)#localdir /pcmcia0/blksts
```

Related Commands

limit
mkdir

receiver

receiver *ip-address* {**primary** | **secondary**} [**mechanism** {**tftp** | **ftp**}] **login** *name* {**password** *passwd* | **nopassword**} [**passive**]

no receiver *ip-address*

Purpose

Specifies the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) servers where remote bulk statistics files are stored.

Command Mode

bulkstats configuration

Syntax Description

ip-address	IP address of the bulkstats receiver.
primary	Specifies that the bulkstats receiver is the primary receiver.
secondary	Specifies that the bulkstats receiver is the secondary receiver.
mechanism	Optional. Sets the file transfer method.
tftp	Specifies that the file transfer method is TFTP.
ftp	Specifies that the file transfer method is FTP.
login *login-name*	Login name to be entered.
password *passwd*	Password to be entered with the login name.
nopassword	Specifies that a password is not required with the login name.
passive	Enables passive mode.

Default

The file transfer method is TFTP.

Usage Guidelines

Use the **receiver** command to specify the FTP or TFTP servers where remote bulk statistics files are stored. If a transfer to the primary receiver fails, a transfer to the secondary receiver is immediately attempted. If transfer to the secondary receiver fails, the Subscriber Management System (SMS) device re-attempts a transfer in five minutes. Retries continue every five minutes until a transfer is successful.

Use the **no** form of this command to delete a previously configured receiver. If you use this command while bulkstats collection is running, no data is transmitted to receivers until a new receiver is defined. If a bulkstats limit is defined, old sample data might be overwritten or lost when the bulkstats data file fills up.

Examples

The following example identifies the server at IP address 10.10.1.34 as the primary bulkstats receiver:

```
[local]RedBack(config-bulkstats)#receiver 10.10.1.34 primary
```

Related Commands

remotefile
show bulkstats
transfer-interval

remotefile

remotefile format *format-string* [*AOS-variable* [*AOS-variable ...*]]

no remotefile format

Purpose

Specifies the format of the bulkstats collection files stored on remote File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFPT) servers.

Command Mode

bulkstats configuration

Syntax Description

format-string String used to format the filename. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. The following special-character sequences are supported:

\n—Creates a new line

%s—A character string|

%d—An integer in decimal (base 10)

%u—An unsigned integer in decimal (base 10)

%x—An integer in hexadecimal format (base 16)

%%—Gets replaced by a single % character in the output

AOS variable Optional. Access Operating System (AOS) variable. The following statistics can be used:

date—Today's date in YYYYMMDD format (string)

epochtime—Time of day in epoch format (seconds since January 1, 1970); integer

hostname—Hostname as specified in the configuration file (string)

sysuptime—System uptime in seconds (integer)

timeofday—Time of day in HHMMSS format (using a 24-hour clock); string

Default

None

Usage Guidelines

Use the **remotefile** command to specify the format of the bulkstats collection files stored on remote FTP or TFTP servers. When using TFTP as the transfer method, the remote file must exist on the TFTP server before data transmission starts. Most TFTP implementations do not allow clients to create files.

Use the **no** form of this command to delete information about the format of the remote file used to store bulkstats information. Bulkstats collection stops until the **remotefile** command is entered again.

Example

The following example sets the filename `isp` where the bulkstats data is to be stored. When the data is transferred to the TFTP host, it uses this filename appended to /tftpboot:

```
[local]RedBack(config-bulkstats)#remotefile format "isp/%s.%s" hostname date
```

The file will be called /tftpboot/isp/*hostname*.*YYYYMMDD* where the *hostname* argument is the name configured for the Redback device and the *YYYYMMDD* argument is the year, month, and day of transfer.

Related Commands

receiver
show bulkstats

sample-interval

sample-interval *minutes*

default sample-interval

Purpose

Specifies the interval between the collocation of bulk statistics samples.

Command Mode

bulkstats configuration

Syntax Description

minutes	Interval, in minutes, between samples. The range of values is 5 to 525,600 minutes (one year). The default value is 15.

Default

The sampling interval is 15 minutes.

Usage Guidelines

Use the **sample-interval** command to specify the interval between the collection of bulk statistics samples. Setting the sampling interval so that transfers occur often can decrease the Subscriber Management System (SMS) device's CPU performance.

Use the **default** form of this command to return the sampling interval to 15 minutes.

Examples

The following example sets the sampling interval to `30` minutes:

```
[local]RedBack(config-bulkstats)#sample-interval 30
```

Related Commands

transfer-interval

schema

schema *name* **format** *format-string* [*AOS-variable* [*AOS-variable* ...]]

no schema *name*

Purpose

Defines the schema for the contents of the bulkstats collection file for system-wide statistics.

Command Mode

bulkstats configuration

Syntax Description

name Name of the schema. Can be no more than 19 characters in length.

format-string String used to format the file name. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. Table 43-3 describes the special-character sequences.

AOS-variable Optional. Access Operating System (AOS) variable. Separate the variables with a space. Table 43-4 lists the variables. Supported variables vary according to product platform.

The special-character sequences described in Table 43-3 are supported:

Table 43-3 Format String Special-Character Sequences

Syntax	Description
\n	Creates a new line
%s	A character string
%d	An integer in decimal (base 10)
%u	An unsigned integer in decimal (base 10)
%x	An integer in hexadecimal format (base 16)
%%	Gets replaced by a single % character in the output

Table 43-4 lists the AOS variables. Supported AOS variables vary according to configuration mode.

Table 43-4 AOS Variables Used with schema Command

AOS Variable	Type	Description
ce_free_user_mem	Integer	Available Control Engine (CE) module memory
ce_total_user_mem	Integer	Total CE module memory
cpu1min	Integer	Average CPU usage for the last minute
cpu5min	Integer	Average CPU usage for the last five minutes
cpu5sec	Integer	Average CPU usage for the last five seconds
date	String	Today's date in YYYYMMDD format
epochtime	Integer	Time of day in epoch format (number of seconds since January 1, 1970)
fe_free_user_mem	Integer	Available Forwarding Engine (FE) module memory
fe_total_user_mem	Integer	Total FE memory
hostname	String	System hostname
rcv_dropped	Integer	Total incoming packets dropped
sysuptime	Integer	System uptime in seconds.
timeofday	String	Time of day in HHMMSS format using a 24-hour clock
total_subscribers	Integer	Total number of active subscribers across all contexts
xmt_dropped	Integer	Total transmit packets dropped
xmt_outstanding	Integer	Total packets remaining to be transmitted

Default

None

Usage Guidelines

Use the **schema** command to define the schema for the contents of the bulkstats collection file for system-wide statistics. You can configure multiple schemas using this command. Each schema gathers a different type and format of data. Each of the schemas is used to create a text record that is appended to the bulkstats collection file every sample period.

Use the **no** form of this command to remove the schema.

Examples

The following example creates a schema named `sample`:

```
[local]RedBack(config-bulkstats)#schema sample format “global: %u, %s, %s, host: %s, %u” sysuptime date timeofday hostname cpu5min
```

The result of the `sample` schema looks like:

```
sample: global: 348765, 19980924, 230834, host: isp1, 2%
```

Related Commands

bulkstats schema
schema-dump
schema profile

schema-dump

schema-dump

no schema-dump

Purpose

Writes configured bulkstats schema formats to the bulkstats data file.

Command Mode

bulkstats configuration

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **schema-dump** command to enable the writing of configured bulkstats schema formats to the bulkstats data file. When enabled, the format of each configured schema will be printed at the beginning of the bulkstats data file.

Use the **no** form of this command to disable the writing of schema formats to the bulkstats data file.

Examples

The following example writes the configured bulkstats schema formats to the bulkstats data file:

```
[local]RedBack(config-bulkstats)#schema-dump
```

Related Commands

bulkstats schema
schema
schema profile

schema profile

schema profile port *name* **format** *format-sting* [*AOS-variable* [*AOS-variable*...]]

no schema profile port *name*

Purpose

Defines a schema profile that can be applied to multiple ports.

Command Mode

global configuration

Syntax Description

name	Name of the schema. Can be no more than 19 characters in length.
format *format-string*	String used to format the output of the schema. String definitions follow the C programming language printf() function syntax. The string must be enclosed in quotation marks. Table 43-5 describes the special-character sequences
AOS-variable	Optional. Access Operating System (AOS) variable for which data will be collected. Separate the variables with a space. Table 43-6 lists the supported AOS variables.

The special-character sequences described in Table 43-5 are supported:

Table 43-5 Format String Special-Character Sequences

Syntax	Description
\n	Creates a new line
%s	A character string
%d	An integer in decimal (base 10)
%u	An unsigned integer in decimal (base 10)
%x	An integer in hexadecimal format (base 16)
%%	Gets replaced by a single % character in the output

Table 43-6 lists the supported AOS variables:

Table 43-6 AOS Variables Used with schema profile Command

AOS Variable	Type	Description
description	String	Description of port
epochtime	Integer	Time of day in epoch format (number of seconds since January 1, 1970)
inoctets	Integer	Number of octets received on this circuit
inpackets	Integer	Number of packets received on this circuit
mcast_inoctets	Integer	Number of multicast octets received on this circuit
mcast_inpackets	Integer	Number of multicast packets received on this circuit
mcast_outoctets	Integer	Number of multicast octets sent on this circuit
mcast_outpackets	Integer	Number of multicast packets sent on this circuit
outoctets	Integer	Number of octets sent from this circuit
outpackets	Integer	Number of packets sent on this circuit
port	Integer	Port number on the I/O module
portspeed	Integer	Port speed in kbps
porttype	String	Port type
rcv_dropped	Integer	Receive packets dropped
slot	Integer	Slot number in the SMS device
sysuptime	Integer	System uptime in seconds
xmt_dropped	Integer	Transmit packets dropped
xmt_outstanding	Integer	Transmit packets outstanding

Default

None

Usage Guidelines

Use the **schema profile** command to define a schema profile that can be applied to one or more ports. To apply the schema to ports, use the **bulkstats schema** command in port configuration mode.

Use the **no** form of this command to delete the specified bulkstats schema profile. If you delete a schema profile that is referenced by one or more port configurations, an error message will be displayed in the bulkstats data file.

Examples

The following example defines a schema profile named `test-profile` and applies the profile to an Asynchronous Transfer mode (ATM) port:

```
[local]RedBack(config)#schema profile port test-profile format “%d/%d desc: %s” slot
port description
[local]RedBack(config)#port atm 4/0
[local]RedBack(config-port)#bulkstats schema atm-schema profile test-profile
```

Related Commands

bulkstats schema—port configuration mode
schema-dump

show bulkstats

show bulkstats [**collection**]

Purpose

Displays parameters associated with the transmission of bulkstats data.

Command Mode

operator exec

Syntax Description

collection	Optional. Specifies that the collection file in its current state is to be shown, rather than the configuration.

Default

Displays bulkstats configuration information.

Usage Guidelines

Use the **show bulkstats** command to display current bulkstats configuration and transfer status, including:

- IP address of primary receiver
- IP address of secondary receiver
- Transfer mechanism to primary receiver
- Transfer mechanism to secondary receiver
- Time of last successful transfer
- IP address of receiver for last successful transfer
- Time of last attempted transfer
- Time of next transfer
- Size (in bytes) of last bulkstats collection file
- Files transmitted during last transfer

Use the **show bulkstats collection** command to debug schema definitions. This command is only available when bulkstats is disabled.

Examples

The following example displays bulk statistics information:

```
[local]RedBack>show bulkstats

Primary receiver: 198.168.145.99 via tftp
Secondary receiver: 198.168.147.31 via tftp
Last successful transfer to 198.168.145.99 at WED MAR 10 14:55:03 1999
Transferred 1019 bytes into
"tftp:/198.168.145.99/bulkstats/redback.dat".
Last transfer attempt WED MAR 10 14:58:47 1999
Next transfer attempt MON MAR 15 09:06:58 1999
```

The following example displays bulk statistics collection information:

```
[local]RedBack(config)>show bulkstats collection

enet0: (454) 0/0 (null) 4632 2a 36 1
hssi30: (454) 3/0 (null) 0 0 0 0
hssi31: (454) 3/1 (null) 0 0 0 0
atm50: (454) 5/0 (null) 0 0 0 0
atm51: (454) 5/1 (null) 0 0 0 0
```

Related Commands

bulkstats collection
receiver
remotefile

transfer-interval

transfer-interval *minutes*

default transfer-interval *minutes*

Purpose

Specifies interval after which bulkstats data is uploaded to File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) servers.

Command Mode

bulkstats configuration

Syntax Description

minutes	Transfer interval in minutes. The range of values is 5 to 525,600 minutes (one year). The default value is 60.

Default

The interval is 60 minutes.

Usage Guidelines

Use the **transfer-interval** command to specify the interval after which bulkstats data is uploaded to FTP or TFTP servers. Use the **bulkstats force transfer** command to force an immediate transfer.

Use the **default** form of this command to return the transfer interval to 60 minutes.

Example

The following example specifies that bulkstats data is transferred to receivers every `180` minutes:

```
[local]RedBack(config-bulkstats)#transfer-interval 180
```

Related Commands

bulkstats force transfer
transfer-interval

Logging Commands

This chapter describes the commands used to configure system event logging.

For overview information, a description of the tasks used to configure system event logging, and for configuration examples, see the "Configuring Logging" chapter in the *Access Operating System (AOS) Configuration Guide*.

log checkpoint

log checkpoint

Purpose

Exchanges the active and inactive logs.

Command Mode

administrator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **log checkpoint** command to exchange the active and inactive system event log buffers. The active log becomes the inactive log, allowing it to be examined without its data being overwritten. The active buffer is circular in nature, in that newer messages overwrite older messages after the buffer is filled. The previous inactive log is cleared, and then becomes the active log.

Examples

In the following example, the user checkpoints the log:

```
[local]RedBack#log checkpoint

Checkpointing the Forwarding Engine log: succeeded.
Checkpointing the Control Engine log: succeeded.
```

Related Commands

save log
show log

logging console

logging console [**circuit** {*slot/port* [{*vpi vci* | [*hdlc-channel*] *dlci*}] | **lac** *vcn* | **lns** *vcn* | **pppoe** [*cm-slot*-]*session-id*} [**only**]]

no logging console

Purpose

Enables event logging to the console.

Command Mode

global configuration

Syntax Description

circuit	Optional. Used to select events for a specific circuit.
slot/port	Slot and port used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay ports. The range of slot values is 0 to 31. The range of port values is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI) used with ATM ports. The VPI range of values is 0 to 255. For ATM T1 modules, the VCI range of values is 1 to 1,023; for ATM DS-3 version 1 modules, the VCI range of values is 1 to 2,047; for ATM OC-3 version 1 modules, the VCI range of values is 1 to 4,095; for all ATM version 2 modules, the VCI range of values is 1 to 65,535.
hdlc-channel	Name of the HDLC channel in the case for a channelized DS-3 port. This argument is required for channelized DS-3 modules and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) used with Frame Relay ports. The range of values is 16 to 991.
lac *vcn*	Layer 2 Tunneling Protocol Access Controllers (LAC) virtual circuit number (VCN). The range of values is 0 to 65,534.
lns *vcn*	Layer 2 Tunneling Protocol Network Services (LNS) virtual circuit number (VCN). The range of values is 0 to 65,534.
pppoe [*cm-slot*-]*session-id*	Point-to-Point Protocol over Ethernet (PPPoE) specifications. The *cm-slot* argument is required for Connection Manager (CM) modules only. You must specify the *session-id* argument for all product platforms; the range of values is 1 to 65,534.
only	Optional. Logs events only associated with the circuit specification.

Default

Console logging is disabled.

Usage Guidelines

You can us the **logging console** command to quickly isolate problems. Messages sent to the console can be further constrained through the use of the circuit specification. If you use a circuit-specification without the **only** keyword, all events that match the circuit specification, and all events that have no circuit specification are logged.

Subsequent **logging console** commands supersede the previous **logging console** command.

Use the **no** form of this command to disable event logging to the console.

Examples

The following example enables logging to the console terminal:

```
[local]RedBack(config)#logging console
```

The following example displays how logging can be further constrained through the use of a circuit specification:

```
[local]RedBack(config)#logging console circuit 3/1 3 200 only
```

In this example, only error messages associated with the specified circuit only are written to the console. Without use of the **only** keyword, all messages associated with the circuit *and* messages with no circuit associations are displayed.

Related Commands

terminal monitor

logging filter

logging filter {**console** | **monitor** | **runtime** | **syslog**} {**all** | **global** | *facility*} *level*

default logging filter {**console** | **monitor** | **runtime** | **syslog**} {**all** | **global** | *facility*} *level*

Purpose

Changes the logging filtering level.

Command Mode

global configuration

Syntax Description

console	Specifies the console filter type.
monitor	Specifies the monitor filter type.
runtime	Specifies the runtime filter type.
syslog	Specifies the syslog filter type.
all	Specifies all facilities.
global	Specifies global default for any filters not explicitly configured.

facility Individual facility that can be one of the following:

aaa—Authentication, authorization, and accounting

bgp—Border Gateway Protocol (BGP)

blkst—Bulk statistics

bridge—Bridging

bt8233—Asynchronous Transfer Mode (ATM)/OC-3

cctmgr—Circuit Manager

cecct—Control Engine (CE) Circuit library

cmmain—Connection Manager (CM) system

cmmgr—CM

dec21140—Ethernet drive

envmon—Environmental Monitoring

fec—Forward Engine (FE) Control

femain—FE system

fepkt—FE packet path

fr—Frame Relay protocol

global—Global logging level

gtd—gatedD

ima—Inverse Multiplexing for ATM (IMA)

ip—Internet Protocol

l2tp—Layer 2 Tunneling Protocol (L2TP)

log—Event logger

ospf—Open Shortest Path First (OSPF)

peb20534—Frame Relay device driver

pm4351—Clear-Channel DS-1

portmgr—Port Manager

ppp—Point-to-Point Protocol (PPP)

pppoe—PPP over Ethernet (PPPoE)

rad—Remote Authentication Dial In User Service (RADIUS)

sys—System

tigon—Ethernet Driver

vpn—Virtual Private Networking (VPN)

level — Specifies the logging level for the specified facility. The logging level can be one of the following:

emergency—Log only emergency events

alert—Log alert and more severe events

critical—Log critical and more severe events

error—Log error and more severe events

warning—Log warning and more severe events

notice—Log notice and more severe events

informational—Log informational and more severe events

debug—Log all events, including debug

Default

Table 44-1 describes the default input and output filter levels for each filter type.

Table 44-1 Default Filter Levels

Input Filter	Output Filter
console	debug
monitor	debug
runtime	informational
syslog	notice

Usage Guidelines

Use the **logging filter** command to isolate events from certain facilities in the logs and trim the flow of information. Use this command to filter events placed into the event log (runtime); to filter events displayed by the **show log** command; or to view the filtered output through the console, monitor, or the syslog server of one facility, any facility not explicitly set, or all facilities.

Use the **default** form of this command to set a logging filter back to its default level.

Examples

The following example modifies the severity level for several log facilities:

```
[local]RedBack(config)#logging filter runtime log error
[local]RedBack(config)#logging filter monitor cctmgr debug
[local]RedBack(config)#logging filter monitor fec emerg
[local]RedBack(config)#logging filter syslog ip alert
[local]RedBack(config)#logging filter console pppoe debug
```

Related Commands

show logging

logging syslog

logging syslog {*ip-address* | *hostname*} [**facility** {*name*}] [**circuit** {[*slot/port* {*vpi vci* | [*hdlc-channel*] *dlci*} | **lac** *vcn* | **lns** *vcn* | **pppoe** [*cm-slot-*]*session-id*} **only**]

no logging syslog {*ip-address* | *hostname*}

Purpose

Enables event logging to a remote syslog server.

Command Mode

context configuration

Syntax Description

ip-address	IP address of the target syslog server.
hostname	Hostname of the target syslog server.
facility *name*	Optional. Syslog facility name. The range of values is local0 to local7. The default value is local7.
circuit	Optional. Specifies a circuit.
slot/port	Slot and port number. The range of slot values is 0 to 31. The range of port values is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI) used with Asynchronous Transfer Mode (ATM) circuits. The VPI range of values is 0 to 255. For ATM T1 modules, the VCI range of values is 1 to 1,023; for ATM DS-3 version 1 modules, the VCI range of values is 1 to 2,047; for ATM OC-3 version 1 modules, the VCI range of values is 1 to 4,095; for all ATM version 2 modules, the VCI range of values is 1 to 65,535.
hdlc-channel	High-level Data Link Control (HDLC) channel. Required for channelized DS-3 cards and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) used with Frame Relay. The range of values is 16 to 991.
lac *vcn*	Layer 2 Tunneling Protocol Access Concentrators (LAC) virtual circuit number (VCN). The range of values is 0 to 65,534.
lns *vcn*	Layer 2 Tunneling Protocol Network Servers (LNS) virtual circuit number (VCN). The range of values is 0 to 65,534.

pppoe [*cm-slot*-] *session-id*	Used in Point-to-Point Protocol over Ethernet (PPPoE). The *cm-slot* is required for Connection Manager (CM) modules and not used in any other case. It specifies the CM slot number. You must enter the session ID for all Redback platforms. The session ID range is 1 to 65534.
only	Optional. Logs only events associated with the circuit specification.

Default

Log messages are sent to the syslog server with a facility of local7.

Usage Guidelines

Use the **logging syslog** command to enable sending of syslog messages to the server from within a context.

You can use the *hostname* option only if Domain Name Service (DNS) is enabled via the **ip domain-lookup**, **ip domain-name**, and **ip name-servers** commands. See the "DNS Commands" chapter.

Use the **no** form of this command to disable the sending of syslog messages to the server.

Examples

The following example enables logging to the syslog server at IP address `10.10.3.46` in the `newworld` context:

```
[local]RedBack(config)#context newworld
[local]RedBack(config-ctx)#logging syslog 10.10.3.46
```

In the following example, logging is further constrained to reference only events associated with slot `5`, port `0`, VPI `255`, VCI `2043` and no others. Events are logged with a facility of `local4`.

```
[local]RedBack(config)#context newworld
[local]RedBack(config-ctx)#logging syslog 10.10.3.46 facility local4 circuit 5/0 255
2043 only
```

Related Commands

ip domain-lookup
ip domain-name
ip name-servers
save log
terminal monitor

save log

save log [**active** | **inactive**] [**text**] *url* [**-noconfirm**]

Purpose

Saves one of the internal event log buffers to the flash file system, to a PCMCIA card, or to a remote File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server.

Command Mode

administrator exec

Syntax Description

active	Optional. Writes the currently active internal event log buffer to the file specified by the *url* argument.
inactive	Optional. Writes the currently inactive internal event log buffer to the file specified by the *url* argument.
text	Optional. Saves the event log in plain text.
url	URL. Format varies according to the location of the file.
-noconfirm	Optional. Replaces existing file without asking for confirmation.

Default

The active log is saved if both the **active** and **inactive** keywords are omitted.

Usage Guidelines

Use the **save log** command to save the system event log for later examination.

Saving the active log causes the system event log to perform an automatic checkpoint prior to the save. As a result, the active log becomes the inactive log and the inactive log is initialized and made active. Any information in the inactive log is lost.

When referring to a file on an FTP server, the URL takes the following form, where the *username*[**:***passwd*] construct specifies the user and an optional password. *A.B.C.D* is the IP address of the FTP server. The **passive** keyword specifies a passive FTP transaction:

ftp://*username*[**:***passwd*]*@A.B.C.D*[/*directory*]/*filename.ext* **passive**

When referring to a file on a TFTP server, the URL takes the following form, where *A.B.C.D* is the IP address of the TFTP server:

tftp://*A.B.C.D*[/*directory*]/*filename.ext*

When referring to a file on the local file system, the URL takes the following form, where the *device* argument can be **flash**, **pcmcia**, or **pcmcia1**:

[**file:**]*/device*[*/directory*]*/filename.ext*

Examples

In the following example, the user writes a copy of the active log to a file called `log.sav` located in the root directory of the system's flash memory:

```
[local]RedBack#save log active file:/flash/log.sav
```

Related Commands

logging syslog
show log

show log

show log [{**active** | **inactive** | *url*} [**since** *start-time* [**until** *end-time*]] [**level** *level*] [**circuit** {*slot/port* [{*vpi vci* | [*hdlc-channel*] *dlci*}] | **lac** *vcn* | **lns** *vcn* | **pppoe** [*cm-slot-*]*session-id*} [**only**]]

Purpose

Displays the system event log.

Command Mode

operator exec

Syntax Description

active	Optional. Specifies that the active log is displayed.
inactive	Optional. Specifies that the inactive log is displayed. If the system restarts as a result of a system error, the active log is moved to the inactive log. If the system was restarted normally, the inactive log is initially blank.
url	URL of the file to be displayed, rather than the active or inactive log. See the "Usage Guidelines" section for details.
since *start-time*	Optional. Only events that happened after the specified time are displayed. This option is useful for seeing the last portion of a log.
until *end-time*	Optional. Only events prior to the timestamp are to displayed.
level *level*	Optional. Only events of the specified level or higher are displayed.
circuit	Optional. Specifies that only events for the circuit are displayed.
slot/port	Slot and port number. Used with Ethernet, Asynchronous Transfer Mode (ATM), and Frame Relay ports. The range of values for the *slot* argument is 0 to 31. The range of values for the *port* argument is 0 to 7.
vpi vci	Virtual path identifier (VPI) and virtual channel identifier (VCI). The range of values for the *vpi* argument is 0 to 255. For the *vci* argument, the range of values depends on the I/O module. For ATM T1 modules, the range of values is 1 to 1,023; for ATM DS-3 version 1 modules, the range of values is 1 to 2,047; for ATM OC-3 version 1 modules, the range of values is 1 to 4,095; for all ATM version 2 modules, the range of values is 1 to 65,535.
hdlc-channel	High-Level Data Link Control (HDLC) channel. Required for channelized DS-3 cards and not allowed in any other case.
dlci	Data-link connection identifier (DLCI) range is 16 to 991. Used with Frame Relay ports.

lac *vcn*	Layer 2 Tunneling Protocol Access Controller (LAC) virtual circuit number (VCN). The range of values is 0 to 65,534.
lns *vcn*	Layer 2 Tunneling Protocol Network Service (LNS) virtual circuit number (VCN). The range of values is 0 to 65,534.
pppoe [*cm-slot-*]*session-id*	Point-to-Point Protocol over Ethernet (PPPoE). The *cm-slot* argument is required for Connection Manager (CM) modules and not used in any other case. It specifies the CM slot number. The session ID must be entered for all Redback platforms. The session ID range of values is 1 to 65,534.
only	Optional. Specifies that messages with no circuit association are not displayed.

Default

None

Usage Guidelines

Use the **show log** command to display the system event log. When referring to a file on a File Transfer Protocol (FTP) server, the URL takes the following form, where *username*[**:***passwd*] construct specifies the user and an optional password. *A.B.C.D* is the IP address of the FTP server. The **passive** keyword specifies a passive FTP transaction.

ftp://*username*[:*passwd*]@*A.B.C.D*[/*directory*]/*filename.ext* **passive**

When referring to a file on a Trivial File Transfer Protocol (TFTP) server, the URL takes the following form, where *A.B.C.D* is the IP address of the TFTP server:

tftp://*A.B.C.D*[/*directory*]/*filename.ext*

When referring to a file on the local file system, the URL takes the following form, where the *device* argument can be /**flash,** /**flash/***file* or **/pcmcia0/***file* or **/pcmcia1/***file*:

[**file:**]*/device*[/*directory*]/*filename.ext*

The **since**, **until**, **level**, and **circuit** keywords are only available after specifying the **active** or **inactive** keyword, or the *filename* argument.

Table 44-2 describes the **level** *level* argument options:

Table 44-2 Event Levels

Level	Description
emergency	Logs only emergency events
alert	Logs alert and more severe events
critical	Logs critical and more severe events
error	Logs error and more severe events
warning	Logs warning and more severe events
notice	Logs notice and more severe events
informational	Logs informational and more severe events
debug	Logs all events, including debug

Examples

The following example displays the active system event log:

```
[local]RedBack>show log

MON NOV 24 11:15:17 1997: %FEMAIN-6-INITSTRT: FE initialization started, logger
initialized.
MON NOV 24 11:15:17 1997: %FEMAIN-6-INIT_FIN: FE initialization complete.
MON NOV 24 11:15:17 1997: %IP-6-INI: IP initializing
MON NOV 24 11:15:17 1997: %IP-6-TARPRX: Spawned ArpRx task
MON NOV 24 11:15:17 1997: %IP-6-TSPN_ARP: Spawned ARP timer task
MON NOV 24 11:15:17 1997: %IP-6-TFWD: Spawned ip_fwd task
MON NOV 24 11:15:17 1997: %IP-6-INI_DONE: IP initializing completed
MON NOV 24 11:15:17 1997: %PORTMGR-6-STATECHG: port atm 3/0 state changed to UP
MON NOV 24 11:15:17 1997: %PORTMGR-6-STATECHG: port ethernet 5/1 state changed to UP
```

The following example displays only that portion of the active log that was entered after `11:15` a.m. on `November 24`:

```
[local]RedBack>show log active since 1997:11:24:11:15:15

MON NOV 24 11:15:16 1997: %IP-6-TSPN_ARP: Spawned ARP timer task
MON NOV 24 11:15:17 1997: %IP-6-TFWD: Spawned ip_fwd task
MON NOV 24 11:15:17 1997: %IP-6-INI_DONE: IP initializing completed
MON NOV 24 11:15:17 1997: %PORTMGR-6-STATECHG: port atm 3/0 state changed to UP
MON NOV 24 11:15:17 1997: %PORTMGR-6-STATECHG: port ethernet 5/1 state changed to UP
```

The following example displays all of the informational-level active log messages and messages with a higher severity level:

```
[local]RedBack>show log active level informational

MON NOV 24 11:15:14 1997: %FEMAIN-6-INITSTRT: FE initialization started, logger
initialized.
MON NOV 24 11:15:14 1997: %FEMAIN-6-INIT_FIN: FE initialization complete.
MON NOV 24 11:15:15 1997: %IP-6-INI: IP initializing
MON NOV 24 11:15:15 1997: %IP-6-TARPRX: Spawned ArpRx task
MON NOV 24 11:15:16 1997: %IP-6-TSPN_ARP: Spawned ARP timer task
MON NOV 24 11:15:17 1997: %IP-6-TFWD: Spawned ip_fwd task
MON NOV 24 11:15:17 1997: %IP-6-INI_DONE: IP initializing completed
MON NOV 24 11:15:17 1997: %PORTMGR-6-STATECHG: port atm 3/0 state changed to UP
MON NOV 24 11:15:17 1997: %PORTMGR-6-STATECHG: port ethernet 5/1 state changed to UP
```

The final example displays all of the active log messages with a notice or higher severity level. No output is displayed, because there were no messages in the active log with a notice or higher severity level.

```
[local]RedBack>show log active level notice
```

Related Commands

logging console
logging filter
logging syslog
save log
show logging

show logging

show logging [**filter** [**all** | **console** | **monitor** | **runtime** | **syslog**]]

Purpose

Displays information about logging filters.

Command Mode

operator exec

Syntax Description

filter	Optional. Displays information about all active and configured logging filtering.
all	Optional. Displays all the information about the events logged.
console	Optional. Displays information about the filtering and logging of events to the console.
monitor	Optional. Displays information about the filtering and logging of events to Telnet sessions.
runtime	Optional. Displays information about the filtering and logging of runtime events.
syslog	Optional. Displays information about the filtering and logging of events to syslog servers.

Default

Displays summary information about all events logged since system startup.

Usage Guidelines

Use the **show logging** command to display information about logging filters. If debugging is enabled, debug appears as the active level, and the configured level is displayed in parentheses.

Examples

In the following example, the **show logging** command displays summary information for the system log facility:

```
[local]RedBack>show logging

CE logged 10 events, (5 filtered, 0 rate limited)
  log has not wrapped since system startup at 10:17:18 Sun Jan 18 1998
FE logged 2 events, (0 filtered, 0 rate limited)
  log has not wrapped since system startup at 10:17:18 Sun Jan 18 1998
logging console: not enabled.
logging monitor: not enabled.
logging syslog: not enabled.
```

Related Commands

logging console
logging filter
logging syslog
show log

Part 13

Network Management Services

SNMP and RMON Commands

This chapter describes the commands used to configure Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) features supported by the Access Operating System (AOS).

For overview information, a description of the tasks used to configure, and configuration examples, see the "Configuring SNMP and RMON" chapter in the *Access Operating System (AOS) Configuration Guide*.

debug snmp

debug snmp {**packet** | **pdu**}

no debug snmp {**packet** | **pdu**}

Purpose

Enables the logging of Simple Network Management Protocol (SNMP) debug messages.

Command Mode

administrator exec

Syntax Description

packet	Enables the logging of debugging messages for SNMP packets.
pdu	Enables the logging of debugging messages for the Protocol Data Unit (PDU) field in SNMP packets.

Usage Guidelines

Use the **debug snmp** command to enable the logging of SNMP debug messages. Use the **packet** keyword to log SNMP packet messages. Use the **pdu** keyword to log SNMP PDU messages. Messages are stored in the system log.

You can use the **logging console** or **terminal monitor** commands to display the messages in real time.

Caution Debugging can severely affect system performance. Exercise caution before enabling any debugging on a production system.

Use the **no** form of this command to disable the logging of SNMP debug messages.

Examples

The following example enables the logging of SNMP packets:

```
[local]RedBack#debug snmp packet

16:55:35 13Dec1999:%SNMP-7-PACKET: 155.53.190.110:51260, packet:
0x30 82 01 c7 02 01 00 04 06 70 75 62 6c 69 63 a2
82 01 b8 02 02 0d b7 02 01 00 02 01 00 30 82 01
aa 30 81 be 06 08 2b 06 01 02 01 01 01 00 04 81
b1 52 65 64 42 61 63 6b 20 4e 65 74 77 6f 72 6b
73 20 41 4f 53 20 45 78 70 65 72 69 6d 65 6e 74
61 6c 20 49 6d 61 67 65 20 33 2e 31 2e 33 2e 31
20 5b 74 68 61 74 63 68 65 72 20 31 37 37 5d 2c
20 50 52 4f 44 55 43 54 49 4f 4e 20 42 55 49 4c
44 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20
31 39 39 37 2d 31 39 39 39 20 62 79 20 52 65 64
42 61 63 6b 20 4e 65 74 77 6f 72 6b 73 2c 20 49
6e 63 2e 0a 43 6f 6d 70 69 6c 65 64 20 31 39 39
39 2d 44 65 63 2d 31 33 20 32 32 3a 34 32 3a 32
32 20 47 4d
...
```

The ellipses (`...`) at the end of the output indicates that the packet was larger than the log buffer allows. Data exceeding the limit was not displayed.

PDU information for the packet provides Management Information Base (MIB) variable information. In the following example, the Redback system is named `cybercom1` and the SNMP agent was started `5,506.68` seconds ago.

```
[local]RedBack#debug snmp pdu

16:55:35 13Dec1999:%SNMP-7-PDU: GetRsp, reqId: 3511, errStatus: 0
errIndex: 0, vbcount: 4
16:55:35 13Dec1999:%SNMP-7-VARBIND: name: sysDescr.0, value: RedBack
16:55:35 13Dec1999:%SNMP-7-VARBIND: name: sysUpTime.0, value: 505668
16:55:35 13Dec1999:%SNMP-7-VARBIND: name: sysDescr.0, value: RedBack
16:55:35 13Dec1999:%SNMP-7-VARBIND: name: sysName.0, value: cybercom1
```

Related Commands

logging console
snmp server
terminal monitor

rmon alarm

rmon alarm *index object-id interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *owner-name*]

no rmon alarm *index*

Purpose

Creates a Remote Monitoring (RMON) alarm entry.

Command Mode

global configuration

Syntax Description

index	Index of the RMON alarm entry. Used to identify the alarm.
object-id	Object ID of the Management Information Base (MIB) object to be monitored.
interval	Sampling time in seconds. The range of values is 1 to 2,147,483,647.
absolute	Compares the actual object value against the threshold value.
delta	Compares the difference between successive samples of the object value against the threshold value.
rising-threshold *value*	Value at which an event is triggered by this alarm.
event-index	Optional. Event to be triggered when the threshold value is exceeded.
falling-threshold *value*	Value at which an event is triggered by this alarm.
owner *owner-name*	Optional. Name of the alarm owner.

Default

No RMON alarms are configured.

Usage Guidelines

Use the **rmon alarm** command to create an RMON alarm. You must enable the SNMP server via the **snmp server** command in global configuration mode before using this command. The alarm group periodically takes statistical samples from MIB variables in the managed device and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.

Use the **no** form of this command to remove an RMON alarm from the configuration.

Examples

The following example configures an RMON alarm to trigger if the difference between successive 60-second samples of ipForwDatagrams exceeds 3000000 or is less than 600000:

```
[local]RedBack(config)#rmon alarm 1 ipForwDatagrams.0 60 delta rising-threshold 3000000
event 1 falling-threshold 600000 event 2 owner gold.isp.net
```

Related Commands

rmon event
show snmp
snmp server

rmon event

rmon event *index* [**description** *text*] [**log**] [**owner** *owner-name*] [**trap** *community*]

no rmon event *index*

Purpose

Creates a Remote Monitoring (RMON) event entry.

Command Mode

global configuration

Syntax Description

index	Index of the RMON event entry. Used to identify the event.
description *text*	Optional. Provides a description of the event.
log	Optional. Specifies that the event generates a log message.
owner *owner-name*	Optional. Identifies the owner of the event.
trap *community*	Optional. Sends the Simple Network Management Protocol (SNMP) trap to the specified community.

Default

No RMON events are configured.

Usage Guidelines

Use the **rmon event** command to create an RMON event entry. You must enable the SNMP server via the **snmp server** command in global configuration mode. The event group controls the generation and notification of events from this device. This group consists of the eventTable and the logTable.

Use the **no** form of this command to remove an RMON event from the configuration.

Examples

The following example creates an RMON event that logs a message and sends a trap to the `GoldTrapRcvr` community:

```
[local]RedBack(config)#rmon event1 description “packets per second too high in context gold.isp.net” log trap GoldTrapRcvr owner gold.isp.net
```

Related Commands

rmon alarm
show snmp
snmp server

show snmp

show snmp {**accesses** | **communities** | **contexts** | **notifies** | **server** | **transports** | **views**}

Purpose

Displays Simple Network Management Protocol (SNMP) information.

Command Mode

administrator exec

Syntax Description

accesses	Displays statistics relative to SNMP usage.
contexts	Displays the configured contexts for SNMP access.
communities	Displays the configured SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) communities, read and write privileges, and access strings.
notifies	Displays statistics related to SNMP notifications.
server	Displays the current state of the SNMP daemon and the User Datagram Protocol (UDP) port on which it is currently configured to listen.
transports	Displays configured SNMP targets (notification receivers).
views	Displays the configured Management Information Base (MIB) views.

Default

None

Usage Guidelines

Use the **show snmp** command to display system information related to the configuration or use of SNMP.

Examples

The following example provides sample output from the **show snmp views** command:

```
[local]RedBack#show snmp views

restricted system - included non-volatile active
restricted snmp - included non-volatile active
restricted snmpEngine - included non-volatile active
restricted snmpMPDstats - included non-volatile active
restricted usmStats - included non-volatile active
```

Related Commands

debug snmp
snmp community
snmp engine-id
snmp group
snmp notify-target
snmp server
snmp target
snmp target-parameters
snmp user
snmp view

show snmp server

show snmp server

Purpose

Displays Simple Network Management Protocol (SNMP) server information.

Command Mode

operator exec

Syntax Description

This command has no keywords or arguments.

Default

None

Usage Guidelines

Use the **show snmp server** command to display SNMP server status, statistics, and error information.

Examples

The following example shows sample output for the **show snmp server** command:

```
[local]RedBack>show snmp server

snmp server is listening on port 161
authentication failure traps are enabled
1 packets received
0 bad versions
1 unknown community name
0 bad community uses
0 packets sent
0 too bigs
0 no such names
0 bad values
0 generic errors
```

Related Commands

debug snmp
snmp community
snmp engine-id
snmp group
snmp notify-target
snmp server
snmp target
snmp user
snmp view

snmp community

snmp community *string* [**all-contexts** | **context** *ctx-name*] [**read-only** | **read-write**] [**view** *view-name*]

no snmp community *string*

Purpose

For Simple Network Management Protocol version 1 (SNMPv1) and SNMP version 2c (SNMPv2c), configures the community string used to permit access to Management Information Base (MIB) objects.

Command Mode

global configuration

Syntax Description

string	Alphanumeric string to be used as the community string.
all-contexts	Optional. Creates the community string for each context. Community strings of the form *string@context-name* can be used to access context-specific data.
context *ctx-name*	Optional. Name of the context that contains the specific instances of MIB objects available to the community. The default context is local.
read-only	Optional. Allows authorized management stations to retrieve MIB objects.
read-write	Optional. Allows authorized stations to both retrieve and modify MIB objects.
view *view-name*	Optional. Name of the view that defines the MIB objects available to the community. The default view is *restricted*.

Default

The default context is local. The default access is read-only. The default view is *restricted*.

Usage Guidelines

Use the **snmp community** command to configure the community string used to permit access to MIB objects. This command is used with SNMPv1 and SNMPv2c only. SNMP server capabilities must be enabled via the **snmp server** command in global configuration mode before configuring communities. For SNMP version 3 (SNMPv3), use the **snmp group** and **snmp user** commands instead of this command.

When you create an SNMP community, it is accessible by both SNMPv1 and SNMPv2c. In addition, the AOS automatically creates a group (with the same name as the community string) for both SNMPv1 and SNMPv2c.

Use the **all-contexts** keyword to trigger the automatic generation of community names for all managed contexts. For example, if an SMS device has three configured contexts (local, aol, and uunet), the **snmp community Fred all-contexts** command creates the structured community strings Fred@local, Fred@aol, and Fred@uunet.

In addition to generating community names, this command generates the appropriate entries in the access control tables.

Use the optional **read-only** keyword to let the community monitor management information and the optional **read-write** keyword to enable the monitoring *and* modification of information.

Use the **no** form of this command to remove a community string.

Examples

The following command defines the community `public` to have read-write access to the MIB object in the view `generic`, and triggers the automatic generation of community strings for all contexts:

```
[local]RedBack(config)#snmp community public all-contexts view generic read-write
```

Related Commands

show snmp
snmp server
snmp view

snmp engine-id

snmp engine-id {**local** | **remote** *name*} *id-string*

default snmp engine-id

no snmp engine-id remote *name*

Purpose

Sets the system engine ID for Simple Network Management Protocol (SNMP) version 3.

Command Mode

global configuration

Syntax Description

local	Specifies the local engine ID.
remote *name*	Specifies the remote engine ID. The name can be configured via the **snmp user** command.
id-string	A string of 10 to 64 hexadecimal characters to be used for the engine-id. If necessary, you can use colons as separators after each two hexadecimal characters. The string takes the following form: 00:00:09:e4:00:00:*port*:*ipaddress*, where port contains four hexadecimal characters and the IP address uses eight hexadecimal characters.

Default

The default value for the *engine-id* argument is local. The default value for the *id-string* argument is a 24-character string consisting of the Redback Enterprise Management Information Base (MIB) object identifier, the management IP address, and the User Datagram Protocol (UDP) port.

Usage Guidelines

Use the **snmp engine-id** command to set the engine ID. This command is used with SNMP version 3 only. There is no equivalent for SNMP version 1 or version 2c. The SNMP server must be enabled via the **snmp server** command in global configuration mode before you can configure the engine ID.

Use the **default** form of this command to set the engine ID back to the default value. Use the **no** form of this command to disable the engine ID.

Caution Changing the engine ID invalidates security information for all users using authentication, and requires you to re-enter the **snmp user** and **snmp community** commands.

Examples

The following command configures the SNMP `local` engine-id with an id-string of `0A:01:01:01:AB:CD`:

```
[local]RedBack(config)#snmp engine-id local 0A:01:01:01:AB:CD
```

Related Commands

show snmp
snmp server

snmp group

snmp group *name* [**context** *name* [**exact** | **prefix**]] [**notify** *notify-view*] [**read** *read-view*] [**security-model** {**1** | **2c** | **usm** {**noauth** | **auth**}}] [**write** *write-view*]

no snmp group *name* [**context** *name* [**exact** | **prefix**]] [**notify** *notify-view*]] [**read** *read-view*] [**security-model** {**1** | **2c** | **usm** {**noauth** | **auth**}}] [**write** *write-view*]

Purpose

Configures a Simple Network Management Protocol (SNMP) version 3 group.

Command Mode

global configuration

Syntax Description

name	Name of the group. The string can be up to 32 characters in length.
context *name*	Optional. Name of the context. The default value is the local context.
exact	Optional. Matches only the context exactly as specified by the **context** *name* construct.
prefix	Optional. Matches any context that begins with the **context** *name* argument.
notify *notify-view*	Optional. Name of the view from which notifications are sent to the group.
read *read-view*	Optional. Name of the view to which this group has read access.
security-model	Optional. Specifies the security model to use for the group.
1	Specifies a security model based on SNMP version 1 community strings.
2c	Specifies a security model based on SNMP version 2c community strings.
usm	Specifies a security model based on SNMP users.
auth	Authorizes SNMP users.
no auth	Does not authorize SNMP users.
write *write-view*	Optional. Name of the view to this group has write access.

Default

A group named *initial* is automatically created if needed (for instance, if the **snmp user** command is used without specifying a group). This group uses the user security model with the **noauth** security level, and allows read access to the view named *restricted*. No **write** view or **notify** view is automatically defined. If the **security-model** keyword is not specified, the default security model is **usm** and the default security level is **noauth**.

Usage Guidelines

Use the **snmp group** command to configure an SNMP group. This command is used only with SNMP version 3 to define access parameters for an SNMP group. The SNMP server must be enabled via the **snmp server** command in global configuration mode before you can configure SNMP groups. For SNMP versions 1 and 2c, use the **snmp community** command.

Use the **no** form of this command to remove an SNMP group. If not specified in the **no** form of the command, optional parameters are set to their default values.

Examples

The following command configures an SNMP group named `Admin` that provides authorized read and modify access to the MIB objects defined in a view named `Admin-View`:

```
[local]RedBack(config)#snmp group Admin security-model usm auth context local read
Admin-View write Admin-View
```

Related Commands

show snmp
show snmp server
snmp user
snmp view

snmp notify

snmp notify *notify-name tag-name* [**inform** | **trap**]

no snmp notify *notify-name*

Purpose

Creates a Simple Network Management Protocol (SNMP) notification and tag name.

Command Mode

global configuration

Syntax Description

notify-name	Name of the notification. The string can be up to 32 characters in length.
tag-name	Tag name for the notification. The string can be up to 32 characters in length.
inform	Optional. Indicates that the type of notification is inform, a confirmed notification that requires a response from the SNMP target. If no response is sent within 5 seconds, the inform is sent again. The number of retries is 2.
trap	Optional. Indicates that the type of notification is trap, a nonconfirmed notification.

Default

The notification type is trap.

Usage Guidelines

Use the **snmp notify** command to create an SNMP notification entry and to associate a tag name with the entry. The SNMP server must be enabled via the **snmp server** command in global configuration mode before creating a notification entry. Use this command in conjunction with the **snmp notify-target** command, which references the *tag-name* argument.

Use the **no** form of this command to remove a notification from the configuration.

Examples

The following example associates defines a notify entry with the notify and tag names both set to `V3Traps`:

```
[local]RedBack(config)#snmp notify V3Traps V3Traps trap
```

Related Commands

show snmp
snmp notify-filter
snmp notify-target
snmp server

snmp notify-filter

snmp notify-filter *filter-name oid-tree* {**excluded** | **included**}

no snmp notify-filter *filter-name*

Purpose

Creates a Simple Network Management Protocol (SNMP) notify filter that includes or excludes particular notifications.

Command Mode

global configuration

Syntax Description

filter-name	Name of the notify filter. The string can be up to 32 characters in length.
oid-tree	The object identifier (OID) of the Abstract Syntax Notation One (ASN.1) sub-tree for which the notifications are to be included or excluded.The format is a string of numbers (such as 1.3.6.2.4) or a word (such as system). Replace a single sub-identifier with the asterisk (*) wildcard to specify a sub-tree family; for example 1.3.*.4.
excluded	Excludes the specified OID tree.
included	Includes the specified OID tree.

Default

None

Usage Guidelines

Use the **snmp notify-filter** command to configure an SNMP notify filter that includes or excludes particular notifications. The SNMP server must be enabled via the **snmp server** command in global configuration mode before configuring a notify filter. Use this command in conjunction with the **snmp notify-target** command which references the *filter-name* argument.

Use the **no** form of this command to remove the specified notify filter from the configuration.

Examples

In the following example the notify-filter `F-NO-rpMau` will exclude `rpMauNotifications`:

```
[local]RedBack(config)#snmp notify-filter F-NO-rpMau rpMauNotifications excluded
```

Related Commands

show snmp
snmp notify
snmp notify-target
snmp server

snmp notify-target

snmp notify-target *notify-target-name ip-address* [**address-context** *ctx-name*] [**port** *udp-port*]
tag *tag-list* **parameters** *target-parameters* [**filter** *filter-name*] [**retries** *count*] [**timeout** *seconds*]

no snmp notify-target *notify-target-name*

Purpose

Configures the Simple Network Management Protocol (SNMP) target management station, which receives SNMP notifications.

Command Mode

global configuration

Syntax Description

notify-target-name	Name of the notify target. The string can be up to 32 characters in length. Use the name specified via the **snmp notify** command.
ip-address	IP address of the management station to receive the notifications.
address-context *ctx-name*	Optional. Name of the context from which the notifications are sent. The default context is local.
port *udp-port*	Optional. User Datagram Protocol (UDP) port used to send the notifications to the target. The range of values is 1 to 65,535. The default value is 162.
tag *tag-list*	List of notification tag names, separated by commas. No spaces are allowed in the list. Tag names are configured via the **snmp notify** command.
parameters *target-parameters*	Name of the target-parameters for this target. Use the name specified via the **snmp target-parameters** command.
filter *filter-name*	Optional. Name of the filter to be applied to the target. Use the name specified via the **snmp notify-filter** command.
retries *count*	Optional. Number of times to retry when sending an inform notification. The range of values is 0 to 255. The default value is two.
timeout *seconds*	Optional. Number of seconds to wait for a reply when an inform notification is sent. The range of values is 0 to 2,147,483,647; the default is five.

Default

The UPD port is 162. The context is local. The timeout value is five seconds. The number of retries is two.

Usage Guidelines

Use the **snmp notify-target** command to configure the SNMP target management station that receives SNMP notifications. The SNMP server must be enabled via the **snmp server** command in global configuration mode before you can configure the target management station.

The **snmp target** and the **snmp notify-target** commands are mutually exclusive. The **snmp target** command is equivalent to the set of **snmp notify-target**, **snmp notify**, **snmp target-parameters**, and **snmp group** (only if the **notify** *notify-view* construct has not been set) commands, where a number of parameters default to particular values. The parameters that are set to their default values by the **snmp target** command are notifyName, targParmName, tag, tagList, seconds, and count.

Before specifying the *notify-target-name* argument, you must first configure the name via the **snmp notify** command. Before specify the *target-parameters* argument, you must first configure the name of the set of parameters configured via the **snmp target-parameters** command. Before specifying the **filter** *filter-name* construct, you must first configure the name using the **snmp notify-filter** command.

Use the **no** form of this command to remove a target from the configuration.

Examples

The following command configures the system to send notifications to a target named `Nm-Station1`, IP address `10.3.4.5`, using the tag `Inet-Informs`, parameters named `Param2`, and notify filter `F-NO-rpMau`:

```
[local]RedBack(config)#snmp notify-target Nm-Station1 10.3.4.5 tag Inet-Informs
parameters Param2 filter F-NO-rpMau
```

Related Commands

show snmp
snmp notify
snmp notify-filter
snmp server

snmp server

snmp server [**port** *udp-port*]

no snmp server

Purpose

Enables Simple Network Management Protocol (SNMP) versions 1, 2c, and 3 server capabilities.

Command Mode

global configuration

Syntax Description

port *udp-port*	Optional. Number of the Universal User Datagram Protocol (UDP) port through which the SNMP server receives and sends data. The range of values is 1 to 65,535. The default value is 161.

Default

SNMP server capabilities are disabled. The UDP port is 161.

Usage Guidelines

Use the **snmp server** command to enable the SNMP server. The optional **port** parameter can be used to configure the system to send and receive SNMP data on a different UDP port than the default port (161).

Caution If you disable the SNMP server, all SNMP information is removed from the configuration.

Note This command is also described in Chapter 46, “Web Management Commands.”

Examples

The following command enables the SNMP server on the default UDP port 161:

```
[local]RedBack(config)#snmp server
```

Related Commands

show snmp server
snmp community
snmp engine-id
snmp group
snmp notify-target
snmp server
snmp target
snmp user
snmp view

snmp target

snmp target *target-name ip-address* [**address-context** *ctx-name*] [**port** *udp-port*] [**security-name** *security-name*] [**group** *group-name*] [**inform** | **trap**] [**security-level** {**auth** | **noauth** | **priv**}]}] [**version** {**1** | **2c** | **3**}] [**view** *notify-view*]

no snmp target *target-name*

Purpose

Configures the Simple Network Management Protocol (SNMP) target management station that receives SNMP notifications.

Command Mode

global configuration

Syntax Description

target-name	Name of the target management station. The string can be up to 32 characters in length.
ip-address	IP address of the target management station.
address-context *ctx-name*	Name of the context from which notifications are sent.
port *udp-port*	Optional. User Datagram Protocol (UDP) port from which to send notifications. The default port is 162.
security-name *security-name*	Community name specified via the **snmp community** command (SNMPv1 or SNMPv2c) or username specified via the **snmp user** command (SNMPv3).
group *group-name*	Optional. Identifies the group of users that receive notifications on the target management station. The group name is specified via the **snmp community** command (SNMPv1 or SNMPv2c), or via the **snmp group** command (SNMP v3). The default group is *initial*.
inform	Optional. Indicates that the type of notification is inform, a confirmed notification that requires a response from the SNMP target. If no response is sent within five seconds, the inform is sent again. The number of retries is two seconds.
trap	Optional. Indicates that the type of notification is trap, a nonconfirmed notification.

security-level	Optional. Specifies the security level for the SNMP target.
auth	Provides authentication.
noauth	Does not provide authentication.
priv	Enforces privacy (SNMPv3 authorization privilege level support).
version	Optional. Specifies the SNMP version for the target.
1	Specifies SNMP version 1.
2c	Specifies SNMP version 2c.
3	Specifies SNMP version 3.
view *notify-view*	Optional. Identifies the SNMP notify view. The default view is *restricted*.

Default

The default SNMP version is version 3. The default group that is created by the system is *initial*. The default notification view created by the system is *restricted*. The default notification type is trap.

Usage Guidelines

Use the **snmp target** command to configure the SNMP target management station that receives SNMP notifications. You must enable the SNMP server via the **snmp server** command in global configuration mode before you can define an SNMP target.

The **snmp target** and the **snmp notify-target** commands are mutually exclusive. The **snmp target** command is equivalent to the set of **snmp notify-target**, **snmp notify**, **snmp target-parameters**, and **snmp group** (only if the **notify** *notify-view* construct has not been set) commands, where a number of parameters default to particular values. The parameters that are set to their default values by the **snmp target** command are notifyName, targParmName, tag, tagList, seconds, and count.

For SNMPv1 and SNMPv2c only, these restrictions apply to the **snmp target** command:

- **security-level** {**auth** | **no auth** | **priv**} keywords—There is no authorization provided in SNMPv1 and SNMPv2c. You must specify the **noauth** keyword for SNMPv1 and SNMPv2c. For SNMPv3 you can specify any of the three keywords. Enforcing either the **auth** or **priv** keyword applies authorization or privacy support to the designated SNMP target; use the **no auth** keyword to apply neither authorization nor privacy support.
- **group** *name* construct—Specifies the community name as the group name for SNMPv1 and SNMPv2c. The community name is created using the **snmp community** command.
- [**trap** | **inform**] keyword options—SNMPv1 supports traps only.

Use the **no** form of this command to remove an SNMP target.

Examples

The following example creates an SNMP target named `NM-Station1`, at IP address `198.164.190.110`, to receive SNMPv2c traps from the view named `InetView` using a security and group name of `Admin`:

```
[local]RedBack(config)#snmp target NM-Station1 198.164.190.110 security-name Admin
group Admin version 2c view InetView traps
```

Related Commands

show snmp
snmp community
snmp group
snmp target-parameters
snmp server
snmp user
snmp view

snmp target-parameters

snmp target-parameters *parameter-name* **security-name** *security-name* [**version** {**1** | **2c** | **3**}] [**security-level** {**auth** | **noauth** | **priv**}]

no snmp target-parameters *parameter-name*

Purpose

Configures the set of parameters to be applied to a Simple Network Management Protocol (SNMP) target.

Command Mode

global configuration

Syntax Description

parameter-name	Name of the target parameter set.
security-name *security-name*	Community name specified via the **snmp community** command (SNMPv1 or SNMPv2c) or user name specified via the **snmp user** command (SNMPv3).
version	Optional. Specifies the SNMP version to use to send the notifications.
1	Specifies SNMP version 1.
2c	Specifies SNMP version 2c.
3	Specifies SNMP version 3c.
security-level	Optional. Security level to be applied to an SNMP target.
auth	Provides authorization.
noauth	Does not provide authorization.
priv	Enforces authentication privilege level support in SNMP version 3.

Default

None

Usage Guidelines

Use the **snmp target-parameters** command to configure the set of parameters to be applied to an SNMP target. You must enable the SNMP server via the **snmp server** command in global configuration mode before you can configure target parameters. Use this command in conjunction with the **snmp notify-target** command.

For the **security-level** {**auth** | **no auth | priv**} keywords, there is no authorization provided in SNMPv1 and SNMPv2c. You must specify the **noauth** keyword for SNMPv1 and SNMPv2c. For SNMPv3, you can specify any of the three keywords. Enforcing either the **auth** or **priv** option applies authorization or privacy support to the designated SNMP target; use the **no auth** option to apply neither authorization nor privacy support.

Use the **no** form of this command to remove the specified target parameter information from the configuration.

Examples

The following command configures a set of parameters named `Param2` that include the security name `ADMIN`, and specify the SNMPv3 protocol using authorization:

```
[local]RedBack(config)#snmp target-parameters Param2 security-name ADMIN version 3
security-level auth
```

Related Commands

show snmp
snmp community
snmp notify
snmp notify-filter
snmp notify-target
snmp server
snmp target
snmp user

snmp user

snmp user *name* [**engine** *name*] [**group** *name*] [**security-model** {**1** | **2c** | **usm** {**noauth** | **md5** | **sha**}} [{**password** *auth-pwd* [**des56** *priv-pwd*] [**key** *auth-key*] [**encoded base64**] [**des56** *des-key*]}]

no snmp user *name* [**engine** *name*] [**group** *name*] [**security-model** {**1** | **2c** | **usm** {**noauth** | **md5** | **sha**}} [{**password** *auth-pwd* [**des56** *priv-pwd*] [**key** *auth-key*] [**encoded base64**] [**des56** *des-key*]}]

Purpose

Configures a Simple Management Network Protocol (SNMP) version 3 user.

Command Mode

global configuration

Syntax Description

name	Name of the SNMP user, up to 32 characters long.
engine *name*	Optional. Name of the remote engine previously configured via the **snmp engine-id** command.
group *name*	Optional. Name of the group the user belongs to, up to 32 characters long.
security-model	Optional. Specifies the type of security model.
1	Specifies SNMP version 1.
2c	Specifies SNMP version2c.
usm	Specifies the User-Based Security Model (USM) for SNMP version 3.
noauth	Specifies no authentication.
md5	Specifies MD5 authenticating.
sha	Specifies SHA authentication.
password *auth-pwd*	Authentication password. Specified only for the user security model, with authentication.
des56 *priv-pwd*	Optional. DES56 privileged password in text string form.
key *auth-key*	Authentication key value. Specified only for the user security model, with authentication.
encoded base64	Optional. Specifies that the key provided in the command is already in a base-64 encoded form. If you omit this keyword, the system encodes the *auth-key* argument prior to storing it in the configuration.
des56 *des-key*	Optional. Des56 encrypted key value.

Default

The default security model is usm, with no authorization.

Usage Guidelines

Use the **snmp user** command to configure an SNMP version 3 user. You must first enable the SNMP server via the **snmp server** command in global configuration mode before configuring a user.

Use the **no** form of this command to remove an SNMP user.

Examples

The following command creates an SNMP user named `Admin` that is part of the group named `Group4`, and uses MD5 authentication with the password `xyzzy`, and an optional `des56` password `loopy`:

```
[local]RedBack(config)#snmp user Admin group Group4 security-model usm md5 password
"xyzzy" des56 loopy
```

Related Commands

show snmp
snmp engine-id
snmp group
snmp server
snmp view

snmp view

snmp view *name oid-tree* {**excluded** | **included**}

no snmp view *name* [*oid-tree*]

Purpose

Configures a Simple Network Management Protocol (SNMP) Management Information Base (MIB) view.

Command Mode

global configuration

Syntax Description

name	Alphanumeric string used as a label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	The object identifier (OID) of the ASN.1 subtree to be included, or excluded, from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
excluded	Excludes the specified OID tree.
included	Includes the specified OID tree.

Default

A default view named *restricted* is enabled when it is referenced, and it provides access to the following MIB groups: system, snmp, snmpEngine, snmpMPDStats, and usmStats.

Usage Guidelines

Use the **snmp view** command to configures an SNMP MIB view. MIB views control which SNMP communities have access to specific MIB objects. You must first enable the SNMP server via the **snmp server** command.

Use the **no** form of this command to remove the specified MIB view entry.

Examples

The following example creates a view that includes all objects in the Internet subtree:

```
[local]RedBack(config)#snmp view everything internet included
```

The following example creates a view that includes only the system group and the interface MIB objects for the port with an value of 6.

```
[local]RedBack(config)#snmp view port6 system included
[local]RedBack(config)#snmp view port6 ifEntry.*.6 included
```

Related Commands

show snmp
snmp community
snmp group
snmp server
snmp user

Web Management Commands

This chapter describes the commands used to enable web access to the Access Operating System (AOS).

For overview information, a description of the tasks used to enable web access, an overview of the capabilities of the Redback web management interface, and for configuration examples, see the "Configuring Web Management" chapter in the *Access Operating System (AOS) Configuration Guide*.

clear http

clear http *session-number*

Purpose

Clears an HTTP session.

Command Mode

operator exec

Syntax Description

session-number	HTTP session number to be cleared. The range of values is 1 to 1,000.

Default

None

Usage Guidelines

Use the **clear http** command to clear an HTTP session. To view HTTP sessions, use the **show administrators** command in operator exec mode.

Examples

The following example clears HTTP session number 2:

```
[local]RedBack>clear http 2
```

Related Commands

show administrators

http server

http server

no http server

Purpose

Enables the administrator to configure and view the Subscriber Management System (SMS) device through a web browser.

Command Mode

global configuration

Syntax Description

This command has no keywords or arguments.

Default

The HTTP server is disabled.

Usage Guidelines

Use the **http server** command to configure and monitor the SMS device through a web browser. Y

Use the **no** form of this command to disable monitoring using a web browser.

Examples

The following example first enables the SNMP server, and then enables the HTTP server:

```
[local]RedBack(config)#http server
```

Related Commands

NetOp Commands

This chapter describes the Access Operating System (AOS) command used to configure the Subscriber Management System (SMS) device NetOp server port.

For overview information, a description of the tasks used to configure support for the NetOp Network Manager product, and for configuration examples, see the "Configuring NetOp Support" chapter in the *Access Operating System (AOS) Configuration Guide*.

For further details on the NetOp Network Manager product, see the *NetOp Network Manager for SMS Installation Guide* and the *NetOp Network Manager for SMS Operations Guide*.

netop server

netop server *port-num*

Purpose

Configure the NetOp server port that is used to communicate with the NetOp Network Manager product.

Command Mode

global configuration

Syntax Description

port-num	TCP port to listen on. The range of values is 0 to 65,535.

Default

None

Usage Guidelines

Use the **netop server** command to configure the Netop server port on the SMS device that is used to communicate with the NetOp Network Manager product. The port number must match the port number specified in the NetOp Network Manager product.

Note To enable the SMS device to operate with the NetOp Network Manager product, you must also enable the SNMP server, configure the network management port, and set up an administrator account on the SMS device. See the commands listed under "Related Commands" and the appropriate chapters in the *Access Operating System (AOS) Configuration Guide*.

Examples

The following enables the NetOp server on port `2001`:

```
[local]RedBack(config)#netop server port 2001
```

Related Commands

administrator
bind interface
port ethernet

show port
shutdown
snmp server

Part 14

Appendixes

Obsolete Commands

The commands listed in Table A-1 should no longer be used in new Access Operating System (AOS) configurations. If possible, support for these commands in existing configuration files will continue. For new configurations, use the commands listed in the “New Commands” column of Table A-1as alternatives.

Table A-1 Obsolete and Replacement Commands

Obsolete Command	New Commands
aaa default-context	**aaa default-domain**
atm pvc default	**atm pvc explicit** **atm pvc on-demand**
bind l2tp-session	**bind session**
circuit creation	**atm pvc explicit** **atm pvc on-demand** **frame-relay pvc explicit** **frame-relay pvc on-demand**
circuit prefix-string	**atm pvc explicit** **atm pvc on-demand** **frame-relay pvc explicit** **frame-relay pvc on-demand**
circuit range	**atm pvc explicit** **atm pvc on-demand** **frame-relay pvc explicit** **frame-relay pvc on-demand**
clear counters	**clear port counters**
clear l2tp group	**clear tunnel**
clear l2tp peer	**clear tunnel** (L2TP) **clear tunnel** (L2F)
frame-relay pvc default	**frame-relay pvc explicit** **frame-relay pvc on-demand**
l2tp-tunnel domain	**tunnel domain** (L2TP) **tunnel domain** (L2F)
l2tp-tunnel name	**tunnel name** (L2TP) **tunnel name** (L2F)

Table A-1 Obsolete and Replacement Commands

Obsolete Command	New Commands
min-sessions	**l2x profile** (L2F) **min-subscribers** (L2F) **profile** (L2F) **l2x profile** (L2TP) **min-subscribers** (L2TP) **profile** (L2TP)
show atm range	None
show frame-relay range	None
snmp manager	**snmp target**

Part 15

Indexes

Commands by Mode Index

A

access control list configuration mode
- deny
  - bridge access control lists, 38-8
  - IP access control lists, 37-16
- deny icmp, 37-18
- deny igmp, 37-21
- deny ip, 37-24
- deny lsap, 38-11
- deny tcp, 37-26
- deny type, 38-13
- deny udp, 37-26
- permit
  - bridge access control lists, 38-8
  - IP access control lists, 37-16
- permit icmp, 37-18
- permit igmp, 37-21
- permit ip, 37-24
- permit lsap, 38-11
- permit tcp, 37-26
- permit type, 38-13
- permit udp, 37-26
- redirect interface next-hop, 37-29
- redirect interface next-hop icmp, 37-34
- redirect interface next-hop ip, 37-39
- redirect interface next-hop tcp, 37-44
- redirect interface next-hop udp, 37-44
- reflexive ftp, 37-50
- reflexive tcp, 37-53
- reflexive tftp, 37-50
- reflexive udp, 37-53

administrator configuration mode
- privilege max, 6-13
- privilege start, 6-14
- timeout, 6-22

administrator exec mode
- bert
  - channelized DS-3 ports, 12-2
  - packet T1 and E1 ports, 15-2
- clear arp-cache, 8-2
- clear bert
  - channelized DS-3 ports, 12-4
  - packet T1 ports, 15-6
- clear bridge table, 21-10
- clear fabric-counters, 42-5
- clear gre, 24-3
- clear ip bgp, 34-9
- clear ip counter, 6-4
- clear ip localhosts, 28-2
- clear ipsec peer, 27-5
- clear lmi-counters, 18-6
- clear pmon
  - channelized DS-3 ports, 12-5
  - packet T1 and E1 ports, 15-7
- clear port counters, 9-9
- clear tunnel
  - L2F, 26-2
  - L2TP, 25-6
- clock set, 5-3
- configure, 4-6, 5-8
- copy, 4-8
- debug aaa, 40-35
- debug all, 42-7
- debug atm, 17-26
- debug bridge span-tree, 21-11
- debug bridge table, 21-13
- debug dhcp, 29-2
- debug frame-relay lmi, 18-10
- debug frame-relay packet, 18-12
- debug hdlc, 9-12
- debug ip all, 42-10
- debug ip arp
  - interfaces, 7-2
  - subscribers, 8-5
- debug ip bgp, 34-13
- debug ip ce-fe, 42-12
- debug ip dns, 28-3
- debug ip host, 42-13

debug ip icmp, 42-15
debug ip igmp, 36-2
debug ip interface, 7-4
debug ip ospf, 33-13
debug ip packet, 42-17
debug ip ppp-proxy-arp, 23-7
debug ip rip, 32-3
debug ip route, 31-4
debug ip routing, 31-6
debug ip secured-arp, 7-6
debug ip sm-cm, 42-19
debug ip tcp, 42-21
debug ip telnet, 3-6
debug ip tftp, 4-11
debug ipsec ike, 27-7
debug ipsec peer, 27-8
debug l2x
L2F, 26-4
L2TP, 25-10
debug ntp, 30-2
debug ppp, 23-2
debug pppoe, 23-5
debug radius, 41-2
debug snmp, 45-2
debug sshd, 3-8
delete, 4-13
directory, 4-15
fabric revert, 4-17
format
DHCP, 29-21
system image and configuration, 4-19
frame-relay-test, 18-44
ip igmp join-group, 36-8
ip igmp leave-group, 36-11
log checkpoint, 44-2
mkdir, 4-21
module extract, 4-23
reload, 4-25
rename, 4-27
rmdir, 4-29
save configuration, 4-31
save log, 44-11
show as-path-access-list, 35-34
show bert
channelized DS-3 ports, 12-20
packet T1 and E1 ports, 15-21
show bridge access-list, 38-15
show bridge address, 21-22
show bridge info, 21-23
show bridge span-tree, 21-24
show bridge table, 21-27
show community-list, 35-35
show configuration, 4-33
show ip access-list, 37-57
show ip dynamic-acl subscriber, 37-59
show ip reflexive-acl, 37-61
show ipsec peer, 27-60
show ipsec stats, 27-62
show pppoe services, 23-52
show route-access-list, 35-36
show service access-list, 39-11
show snmp, 45-8
show te cpu, 27-65
show te performance, 27-67
show te ps, 27-68
show te time, 27-70
show tech
system monitoring, 42-70
sshd keygen, 3-14
telnet, 3-15
All Configuration Modes
end, 2-6
All Modes
? (Help), 2-2
exit, 2-7
ATM profile configuration mode
buffers, 17-14
bulkstats schema
ATM, 17-16
bulkstats, 43-6
clpbit, 17-23
counters, 17-24
radius attribute medium-type
ATM, 17-36
RADIUS, 41-25
shaping, 17-38

B

BGP configuration mode
aggregate-address, 34-4
always-compare-med, 34-7
cluster-id, 34-12
export-non-active, 34-17
group, 34-18
precedence, 34-37
redistribute, 34-41
BGP group configuration mode
accept-med, 34-2
client-to-client, 34-11
default-originate, 34-15
hold-time, 34-20
maximum-prefix, 34-22
maximum-prefix-warn, 34-24
metric-out, 34-26
neighbor, 34-28
nexthop-self, 34-29
no-aggregator-id, 34-31

out-delay, 34-33
passive, 34-35
precedence, 34-37
preference, 34-39
remove-private-AS, 34-43
route-reflector-client, 34-50
throttle, 34-64
ttl, 34-65
BGP peer configuration mode
accept-med, 34-2
allow-bad-routerid, 34-6
enable-peer, 34-16
hold-time, 34-20
maximum-prefix, 34-22
maximum-prefix-warn, 34-24
nexthop-self, 34-29
no-aggregator-id, 34-31
out-delay, 34-33
passive, 34-35
precedence, 34-37
preference, 34-39
remove-private-AS, 34-43
route-map, 34-45
ttl, 34-65
bridge configuration mode
bridge-only, 21-6
forward-time, 21-14
hello-time, 21-16
max-age, 21-17
priority, 21-18
protocol, 21-20
bulkstats configuration mode
header format, 43-10
limit, 43-12
localdir, 43-14
receiver, 43-16
remotefile, 43-18
sample-interval, 43-20
schema, 43-21
schema-dump, 43-24
transfer-interval, 43-30
bypass configuration mode
description, 22-4

C

circuit configuration mode
bind authentication, 20-2
bind auto-subscriber, 20-4
bind bypass, 20-7
bind dot1q, 20-9
bind interface, 20-11
bind l2tp-tunnel, 20-13
bind multi, 20-15
bind session, 20-18
bind subscriber, 20-20
description, 9-14
dot1q pvc, 19-4
ip host, 9-15
mac address, 9-17
context configuration mode
aaa accounting, 40-2
aaa authentication administrator, 40-4
aaa authentication re-try, 40-5
aaa authentication subscriber, 40-7
aaa authorization access-list, 37-3, 40-9
aaa authorization circuit, 40-11
aaa authorization gre, 40-12
aaa authorization tunnel, 40-13
aaa binding, 40-15
aaa delay-start-record, 40-21
aaa hint ip-address, 40-22
aaa max-subscribers, 40-26
aaa min-subscribers, 40-28
aaa update, 40-31
access-list undefined
bridge access control lists, 38-3
IP access control lists, 37-5
administrator, 6-2
as-path access-list, 35-2
bridge, 21-2
bridge access-list, 38-5
bulkstats schema, 43-6
bypass, 22-2
community-list, 35-5
dhcp relay option, 29-8
dhcp relay server, 29-10
domain, 6-7
gre-peer, 24-7
interface
interfaces, 7-9
PPP, 23-9
ip access-group
contexts, 6-9
IP access control lists, 37-9
ip access-list, 37-11
ip bgp-community, 35-7
ip dns-ttl, 28-7
ip domain-lookup, 28-8
ip domain-name, 28-10
ip igmp join-group, 36-8
ip localhost, 28-11
ip maximum-paths, 31-10
ip multicast-routing, 36-19
ip name-servers, 28-13
ip route, 31-12
ipsec key name, 27-33
ipsec peer default, 27-45

ipsec peer name, 27-47
ipsec policy name, 27-50
ipsec proposal crypto name, 27-51
ipsec proposal ike name, 27-52
l2f-peer name, 26-12
l2tp attribute calling-number real-circuit-id, 25-26
l2tp-group name, 25-24
l2tp-peer default, 25-27
l2tp-peer name, 25-29
l2tp-peer unnamed, 25-31
l2x profile
L2F, 26-14
L2TP, 25-35
logging syslog, 44-9
operator, 6-11
ppp keepalive, 23-16
radius accounting algorithm, 41-4
radius accounting deadtime, 41-6
radius accounting max-outstanding, 41-7
radius accounting max-retries, 41-9
radius accounting server, 41-11
radius accounting timeout, 41-13
radius algorithm, 41-15
radius attribute acct-session-id, 41-17
radius attribute calling-station-id, 41-19
radius attribute connect-info, 41-21
radius attribute filter-id, 41-23
radius attribute nas-ip-address, 41-27
radius attribute non-rfc-242, 41-29
radius attribute tunnel password, 41-31
radius deadtime, 41-33
radius max-outstanding, 41-35
radius max-retries, 41-37
radius server, 41-39
radius strip-domain, 41-41
radius timeout, 41-43
route-access-list
extended-access-list-number, 35-17
standard-access-list-number, 35-19
route-map, 35-21
router bgp, 34-47
router igmp-proxy, 36-33
router ospf, 33-33
router rip, 32-20
router-id
BGP, 34-49
OSPF, 33-32
subscriber, 8-23

D

dot1q profile configuration mode
pbit-setting, 19-6
dot1q PVC configuration mode
bind authentication, 20-2
bind interface, 20-11
bind multi, 20-15
bind session, 20-18
bind subscriber, 20-20
description, 19-2

F

Frame Relay profile configuration mode
buffers, 18-2
bulkstats schema
bulkstats, 43-6
Frame Relay, 18-3
counters, 18-8
radius attribute medium-type
Frame Relay, 18-46
RADIUS, 41-25

G

global configuration mode
aaa accounting, 40-2
aaa authentication subscriber, 40-7
aaa default-domain, 40-17
aaa last-resort, 40-24
aaa terse-messages, 40-30
aaa update, 40-31
aaa username-format, 40-33
administrator reserve, 3-2
atm profile, 17-4
banner motd, 5-2
boot configuration, 4-2
boot system, 4-4
bridge station-move verbose, 21-8
bulkstats collection, 43-2
bulkstats mode, 43-5
clock summer-time, 5-4
clock timezone, 5-6
console-break-enable, 3-5
context, 6-5
dhcp preserve-state, 29-6
dot1q profile, 19-3
fabric revert, 4-17
frame-relay profile, 18-34
http server, 46-3
ima enable, 17-31
ima group, 17-32
ip dynamic-acl timeout, 37-13
ip reflexive timeout, 37-15
l2tp eth-sess-idle-timeout, 25-37
l2tp radius auto-group, 25-33
line, 3-11
logging console, 44-3

logging filter, 44-5
netop server, 47-2
ntp mode, 30-4
ntp server, 30-5
port atm, 11-16
port channelized-ds3, 12-19
port ds1, 15-19
port ds3, 13-11
port e1, 15-20
port e3, 13-12
port ethernet, 10-9
port hssi, 14-10
port pos, 16-12
port te, 27-56
ppp multilink enable, 23-19
ppp multilink endpoint-discriminator, 23-21
ppp multilink mrru, 23-23
ppp our-options, 23-24
ppp passive, 23-26
ppp peer-options, 23-28
pppoe services, 23-34
pppoe tag, 23-35
privilege, 5-10
rmon alarm, 45-4
rmon event, 45-6
schema profile, 43-25
service access-list, 39-9
snmp community, 45-12
snmp engine-id, 45-14
snmp group, 45-16
snmp notify, 45-18
snmp notify-filter, 45-20
snmp notify-target, 45-22
snmp server, 45-24
snmp target, 45-26
snmp target-parameters, 45-29
snmp user, 45-31
snmp view, 45-33
system contact, 5-13
system hostname, 5-14
system location, 5-15
tunnel map, 24-25

GRE configuration mode
police, 24-14

GRE peer configuration mode
checksum, 24-2
description, 24-5
rate-limit, 24-16

H

HDLC channel configuration mode
bind authentication, 20-2
bind bypass, 20-7
bind interface, 20-11
bind session, 20-18
bind subscriber, 20-20
bulkstats schema, 43-6
crc, 12-7
description, 9-14
encapsulation, 12-8
invert-data, 12-14
keepalive, 12-15
shutdown, 9-37
speed, 12-30

I

IGMP configuration mode
def-version, 36-4
last-member-query-interval, 36-23
query-interval, 36-25
query-response-interval, 36-27
robustness, 36-29
startup-query-interval, 36-40
unsolicited-report-interval, 36-42
version1-router-interval, 36-44

IGMP proxy router configuration mode
router-igmp-interface, 36-31

IKE proposal configuration mode
cipher, 27-4
hash, 27-16

IMA group configuration mode
clock mode, 17-19
clock source, 17-21
delay-tolerance, 17-28
description, 17-29
frame-length, 17-30
minimum-links, 17-33
ports, 17-34
symmetry, 17-57

interface configuration mode
bridge-group
bridge access control lists, 38-6
bridges, 21-4
description, 7-8
dhcp relay size, 29-12
dhcp server default-lease-time, 29-14
dhcp server filename, 29-15
dhcp server max-lease-time, 29-16
dhcp server next-server, 29-17
dhcp server option, 29-18
dhcp server range, 29-20
ip access-group, 37-9
ip address, 7-11
ip arp arpa, 7-14
ip arp timeout, 7-15
ip igmp, 36-6

ip igmp mode, 36-14
ip ignore-df-bit, 7-16
ip irdp, 31-8
ip lookup host, 7-18
ip mask-reply, 7-20
ip mtu, 7-21
ip pool, 7-22
ip ppp-proxy-arp, 23-11
ip rip interface-cost, 32-5
ip rip listen, 32-7
ip rip receive version, 32-8
ip rip send version, 32-10
ip rip split-horizon, 32-12
ip rip supply, 32-13
ip secured-arp, 7-24
ip source-address, 7-26
IPSec key configuration mode
in, 27-30
out, 27-54
spi in, 27-71
spi out, 27-72
IPSec peer configuration mode
ike auth, 27-17
ike group, 27-18
ike lifetime hard kbytes, 27-19
ike lifetime hard seconds, 27-21
ike lifetime soft kbytes, 27-23
ike lifetime soft seconds, 27-25
ike pre-shared-key, 27-27
ike sa_subnet, 27-28
ip-address local, 27-31
ip-address remote, 27-32
ipsec lifetime hard kbytes, 27-35
ipsec lifetime hard seconds, 27-39
ipsec lifetime soft kbytes, 27-37
ipsec lifetime soft seconds, 27-41
ipsec mode, 27-43
ipsec options, 27-44
ipsec pfs-group, 27-48
proposal crypto, 27-57
proposal ike, 27-59
IPSec policy configuration mode
tunnel ip, 27-73
IPSec proposal configuration mode
ah hash, 27-2
encapsulation-mode, 27-10
esp cipher, 27-12
esp hash, 27-14

L

L2F configuration mode
description, 26-6
domain, 26-8
function, 26-10
local-name, 26-16
max-sessions, 26-18
max-tunnels, 26-20
police, 26-22
profile, 26-24
rate-limit, 26-26
retry, 26-28
session-auth, 26-30
timeout, 26-37
tunnel-auth, 26-39
L2TP configuration mode
description, 25-12
dnis, 25-14
domain, 25-16
ethernet encapsulation, 25-18
ethernet session, 25-19
function, 25-21
ipsec peer, 25-23
ipsec peer name, 27-47
local-name, 25-39
max-sessions, 25-41
max-tunnels, 25-43
police, 25-48
profile, 25-50
rate-limit, 25-52
retry, 25-54
secondary-tunnel-auth, 25-56
session-auth, 25-58
static, 25-77
timeout, 25-79
tunnel-auth, 25-81
tunnel-window, 25-86
L2TP group configuration mode
algorithm, 25-2
deadtime, 25-8
description, 25-12, 25-16
peer-name, 25-46
L2TP peer configuration mode
bulkstats schema
bulkstats, 43-6
L2X profile configuration mode
min-subscribers
L2F, 26-21
L2TP, 25-45
line configuration mode
length, 3-9
width, 3-21

N

NTP configuration mode
slowsync, 30-11

O

operator exec mode
- atm ping, 17-2
- bulkstats force transfer, 43-4
- clear access-list, 37-7
- clear administrator, 42-2
- clear circuit
  - common port, circuit, channel, 9-7
  - system monitoring, 42-3
- clear http, 46-2
- clear port dot1q, 9-11
- clear subscriber
  - subscribers, 8-3
  - system monitoring, 42-6
- clear tty, 3-4
- enable, 2-4
- ping, 42-24
- show administrator reservations, 3-12
- show administrators, 42-26
- show atm counters, 17-40
- show atm multicast, 17-43
- show atm profile, 17-47
- show atm pvc, 17-49
- show bindings, 20-22
- show bulkstats, 43-28
- show bypass, 22-5
- show clock, 5-12
- show cm stats, 42-28
- show cm table, 42-33
- show context, 6-15
- show debugging, 42-35
- show dhcp, 29-23
- show dhcp server lease, 29-26
- show dhcp server sram, 29-28
- show diag, 42-37
- show dot1q counters, 19-7
- show dot1q profile, 19-9
- show dot1q pvc, 19-10
- show envmon, 42-41
- show fabric counters, 42-42
- show fabric table, 42-44
- show fe stats, 42-47
- show frame-relay counters, 18-48
- show frame-relay lmi-config, 18-51
- show frame-relay lmi-errors, 18-53
- show frame-relay lmi-stats, 18-55
- show frame-relay multicast, 18-57
- show frame-relay profile, 18-60
- show frame-relay pvc, 18-62
- show gre counters, 24-18
- show gre info, 24-20
- show gre tunnel counters, 24-22
- show gre tunnel info, 24-23
- show hardware, 42-52
- show hdlc-channel counters, 12-21
- show hdlc-config, 12-23
- show ima group, 17-52
- show ima pmon, 17-54
- show ip arp
  - interfaces, 7-27
  - subscribers, 8-18
- show ip bgp, 34-52
- show ip bgp groups, 34-55
- show ip bgp neighbors, 34-57
- show ip bgp paths, 34-60
- show ip bgp summary, 34-62
- show ip host, 6-17
- show ip igmp, 36-34
- show ip interface, 7-29
- show ip localhosts, 28-15
- show ip ospf, 33-35
- show ip ospf area, 33-37
- show ip ospf border-router, 33-39
- show ip ospf database, 33-41
- show ip ospf interface, 33-45
- show ip ospf neighbor, 33-47
- show ip ospf summary-range, 33-49
- show ip pool, 7-32
- show ip ppp-proxy-arp, 23-39
- show ip route, 31-16
- show ip secured-arp, 7-33
- show ip socket, 42-56
- show ip static-route, 31-19
- show ip traffic
  - contexts, 6-19
  - system monitoring, 42-57
- show l2f counters, 26-32
- show l2f info, 26-35
- show l2tp counters, 25-60
- show l2tp group, 25-67
- show l2tp info, 25-69
- show log, 44-13
- show logging, 44-17
- show memory, 42-59
- show ntp associations, 30-7
- show ntp status, 30-9
- show pmon
  - channelized DS-3 ports, 12-25
  - packet T1 and E1 ports, 15-22
- show port counters, 9-21
- show port diag, 9-29
- show port dot1q, 9-31
- show port info, 9-33
- show port table, 9-35
- show ppp, 23-41
- show ppp multilink, 23-44, 23-46
- show pppoe, 23-48
- show pppoe counters, 23-50

show privilege, 2-8, 6-21
show process, 42-61
show radius counters, 41-45
show route-map, 35-37
show slot, 42-63
show snmp server, 45-10
show sram, 42-64
show stack, 42-66
show subscribers
subscribers, 8-20
system monitoring, 42-67
show t1 info
channelized DS-3 ports, 12-28
packet T1 ports, 15-24
show terminal, 3-13
show username-format, 40-37
show version, 4-35
terminal length, 3-17
terminal monitor, 3-18
terminal width, 3-20
traceroute, 42-72
OSPF area configuration mode
area-sumrange, 33-4
areatype, 33-6
defaultroute, 33-17
nssa-sumrange, 33-21
ospf-interface, 33-23
OSPF configuration mode
area, 33-2
as-sumrange, 33-8
default-originate, 33-15
precedence, 33-25
redistribute, 33-27
spf-timers, 33-52
OSPF interface configuration mode
authentication, 33-10
cost, 33-12
hello-interval, 33-19
retransmit-interval, 33-29
routerdead-interval, 33-30
router-priority, 33-34
transmit-delay, 33-54

P

port configuration mode
8khztiming, 11-2
atm pvc, 17-5
atm pvc explicit, 17-8
atm pvc on-demand, 17-11
bind authentication, 20-2
bind bypass, 20-7
bind interface, 20-11
bind multi, 20-15
bind session, 20-18
bind subscriber, 20-20
buffers, 9-2
bulkstats schema, 43-6
c2byte, 16-2
cablelength
ATM T1 ports, 11-3
packet T1 ports, 15-4
cell-delineation, 11-5
clock-source
ATM ports, 11-6
channelized DS-3 ports, 12-6
clear-channel DS-3, 13-2
packet over SONET, 16-4
packet T1 and E1 ports, 15-8
crc16, 16-5
description
common port, circuit, channel, 9-14
IPSec (TE) ports, 9-14
dot1q pvc, 19-4
encapsulation, 16-6
clear-channel DS-3, 13-3
Ethernet ports, 10-2
HSSI, 14-2
packet T1 and E1 ports, 15-9
fdl
ATM T1 ports, 11-7
packet T1 ports, 15-11
frame-relay auto-detect, 18-14
frame-relay intf-type, 18-16
frame-relay keepalive, 18-18
frame-relay lmi-n391dte, 18-20
frame-relay lmi-n392dce, 18-22
frame-relay lmi-n392dte, 18-24
frame-relay lmi-n393dce, 18-26
frame-relay lmi-n393dte, 18-28
frame-relay lmi-t392dce, 18-30
frame-relay lmi-type, 18-32
frame-relay pvc, 18-35
frame-relay pvc explicit, 18-38
frame-relay pvc on-demand, 18-41
framing
ATM T1 and E1 ports, 11-9
channelized DS-3 ports, 12-11
clear-channel DS-3, 13-5
packet T1 and E1 ports, 15-12
framing sdh, 16-8
hardware-interface, 14-4
hdlc-channel, 12-13
idle-cell, 11-11
invert-data, 15-14
ip host, 10-4
keepalive
clear-channel DS-3, 13-6

HSSI, 14-6
packet T1 and E1 ports, 15-15
length
ATM DS-3 ports, 11-13
channelized DS-3 ports, 12-16
clear-channel DS-3, 13-8
linecode
ATM T1 ports, 11-14
packet T1 ports, 15-17
loopback
ATM ports, 11-15
channelized DS-3 ports, 12-17
clear-channel DS-3, 13-9
Ethernet ports, 10-6
HSSI ports, 14-8
packet over SONET, 16-9
packet T1 and E1 ports, 15-18
medium, 10-7
packet-length, 16-11
police, 9-19
radius attribute medium-type
Ethernet ports, 10-11
RADIUS, 41-25
rate-limit, 9-20
scramble
ATM ports, 11-17
packet over SONET, 16-13
shutdown, 9-37
speed, 15-26
t1, 12-31
timeslot, 15-27
ts16, 15-29
yellow-alarm
ATM T1 and E1 ports, 11-18
packet T1 and E1 ports, 15-30

R

RIP configuration mode
auto-summary, 32-2
network, 32-14
precedence, 32-16
redistribute, 32-18
version, 32-21
route map configuration mode
match as-path, 35-8
match community-list, 35-9
match interface, 35-10
match ip address, 35-11
match ip next-hop, 35-12
match metric, 35-13
match route-type, 35-14
match tag, 35-16
set as-path prepend, 35-23
set community, 35-25
set ip next-hop, 35-27
set local-preference, 35-29
set metric, 35-30
set origin, 35-32
set preference, 35-33

S

service access list configuration mode
deny any, 39-3
deny context, 39-5
deny domain, 39-7
permit any, 39-3
permit context, 39-5
permit domain, 39-7
subscriber configuration mode
bridge-group
bridge access control lists, 38-6
bridges, 21-4
bulkstats schema, 43-6
dhcp max-addrs, 29-4
dns, 28-5
ip access-group, 37-9
ip address, 8-6
ip arp, 8-8
ip multicast max-groups, 36-15
ip multicast receive, 36-17
ip multicast send, 36-21
ip source-validation, 8-10
ip tos-field, 8-11
ipsec tunnel policy, 27-53
outbound password, 8-13
password, 8-14
police, 8-15
port-limit
PPP, 23-13
subscribers, 8-16
ppp compression, 23-15
ppp mtu, 23-18
pppoe client, 23-30
pppoe motm, 23-32
pppoe url, 23-37
rate-limit, 8-17
timeout, 8-25
tunnel domain
L2F, 26-41
L2TP, 25-83
tunnel name
L2F, 26-43
L2TP, 25-85

T

T1 channel configuration mode
clock-source, 12-6
fdl, 12-10
framing, 12-11
loopback, 12-17
yellow-alarm, 12-32
tunnel circuit configuration mode
bind interface, 20-11
ip host, 24-12
tunnel map mode
gre-tunnel, 24-10

Index

Symbols

? (help), 2-2

Numerics

8khztiming, 11-2

A

aaa accounting, 40-2
aaa authentication administrator, 40-4
aaa authentication re-try, 40-5
aaa authentication subscriber, 40-7
aaa authorization access-list
    AAA, 40-9
    IP access control lists, 37-3
aaa authorization circuit, 40-11
aaa authorization gre, 40-12
aaa authorization tunnel, 40-13
aaa binding, 40-15
aaa default-context, A-1
aaa default-domain, 40-17
aaa delay-start-record, 40-21
aaa hint ip-address, 40-22
aaa last-resort, 40-24
aaa max-subscribers, 40-26
aaa min-subscribers, 40-28
aaa terse-messages, 40-30
aaa update, 40-31
aaa username-format, 40-33
accept-med, 34-2
access-list undefined
    bridge access control lists, 38-3
    IP access control lists, 37-5
administrator, 6-2
administrator reserve, 3-2
aggregate-address, 34-4
ah hash, 27-2
algorithm, 25-2
allow-bad-routerid, 34-6
always-compare-med, 34-7
area, 33-2
area-sumrange, 33-4
areatype, 33-6
as-path access-list, 35-2
as-sumrange, 33-8
atm ping, 17-2
atm profile, 17-4
atm pvc, 17-5
atm pvc default, A-1
atm pvc explicit, 17-8
atm pvc on-demand, 17-11
atm vp, 17-14
authentication, 33-10
auto-summary, 32-2

B

banner motd, 5-2
bert
    channelized DS-3 ports, 12-2
    packet T1 and E1 ports, 15-2
    T1 channels, 12-2
bind authentication, 20-2
bind auto-subscriber, 20-4
bind bypass, 20-7
bind dot1q, 20-9
bind interface
    bindings, 20-11
    GRE tunnels, 24-2
bind l2tp-session, A-1
bind l2tp-tunnel, 20-13
bind multi, 20-15
bind session, 20-18
bind subscriber, 20-20
boot configuration, 4-2
boot system, 4-4
bridge, 21-2
bridge access-list, 38-5
bridge-group
    bridge access control lists, 38-6

bridging, 21-4
bridge-only, 21-6
bridge station-move verbose, 21-8
buffers
ATM profile configuration mode, 17-14
Frame Relay profile configuration mode, 18-2
port configuration mode, 9-2
bulkstats collection, 43-2
bulkstats force transfer, 43-4
bulkstats mode, 43-5
bulkstats schema
ATM profile configuration mode
ATM, 17-16
bulkstats, 43-6
context configuration mode, 43-6
Frame Relay profile configuration mode
bulkstats, 43-6
Frame Relay, 18-3
HDLC channel configuration mode
bulkstats, 43-6
common port, circuit, channel, 9-4
L2TP peer configuration mode
bulkstats, 43-6
port configuration mode
bulkstats, 43-6
common port, circuit, channel, 9-4
subscriber configuration mode, 43-6
bypass, 22-2

C

c2byte, 16-2
cablelength
ATM T1 ports, 11-3
packet T1 and E1 ports, 15-4
cell-delineation, 11-5
checksum, 24-2
cipher, 27-4
circuit creation, A-1
circuit prefix-string, A-1
circuit range, A-1
clear access-list, 37-7
clear administrator, 42-2
clear arp-cache, 8-2
clear bert
channelized DS-3 ports, 12-4
packet T1 ports, 15-6
T1 channels, 12-4
clear bridge table, 21-10
clear circuit
common port, circuit, channel, 9-7
system monitoring, 42-3
clear counters, A-1
clear fabric counters, 42-5
clear http, 46-2
clear ip bgp, 34-9
clear ip counter, 6-4
clear ip localhosts, 28-2
clear ipsec peer, 27-5
clear l2tp group, A-1
clear l2tp peer, A-1
clear lmi-counters, 18-6
clear pmon
channelized DS-3 ports, 12-5
packet T1 and E1 ports, 15-7
T1 channels, 12-5
clear port counters, 9-9
clear port dot1q, 9-11
clear subscriber
subscribers, 8-3
system monitoring, 42-6
clear tty, 3-4
clear tunnel
L2F, 26-2
L2TP, 25-6
client-to-client, 34-11
clock mode, 17-19
clock set, 5-3
clock source, 17-21
clock-source
port configuration mode
ATM ports, 11-6
channelized DS-3 ports, 12-6
clear-channel DS-3 and E3 ports, 13-2
packet T1 and E1 ports, 15-8
POS ports, 16-4
T1 channel configuration mode, 12-6
clock summer-time, 5-4
clock timezone, 5-6
clpbit, 17-23
cluster-id, 34-12
community-list, 35-5
configure, 5-8
loading configuration files, 4-6
console-break-enable, 3-5
context, 6-5
copy, 4-8
cost, 33-12
counters
ATM profile configuration mode, 17-24
Frame Relay profile configuration mode, 18-8
crc, 12-7
crc16, 16-5

D

deadtime, 25-8
debug aaa, 40-35

debug all, 42-7
debug atm, 17-26
debug bridge span-tree, 21-11
debug bridge table, 21-13
debug dhcp, 29-2
debug frame-relay lmi, 18-10
debug frame-relay packet, 18-12
debug hdlc, 9-12
debug ip all, 42-10
debug ip arp
  interfaces, 7-2
  subscribers, 8-5
debug ip bgp, 34-13
debug ip ce-fe, 42-12
debug ip dns, 28-3
debug ip host, 42-13
debug ip icmp, 42-15
debug ip igmp, 36-2
debug ip interface, 7-4
debug ip ospf, 33-13
debug ip packet, 42-17
debug ip ppp-proxy-arp, 23-7
debug ip rip, 32-3
debug ip route, 31-4
debug ip routing, 31-6
debug ipsec ike, 27-7
debug ipsec peer, 27-8
debug ip secured-arp, 7-6
debug ip sm-cm, 42-19
debug ip tcp, 42-21
debug ip telnet, 3-6, 7-8
debug ip tftp, 4-11
debug l2x
  L2F, 26-4
  L2TP, 25-10
debug ntp, 30-2
debug ppp, 23-2
debug pppoe, 23-5
debug radius, 41-2
debug snmp, 45-2
debug sshd, 3-8
default-originate
  BGP, 34-15
  OSPF, 33-15
defaultroute, 33-17
def-version, 36-4
delay-tolerance, 17-28
delete, 4-13
deny
  bridge access control lists, 38-8
  IP access control lists, 37-16
deny any, 39-3
deny context, 39-5
deny domain, 39-7
deny icmp, 37-18
deny igmp, 37-21
deny ip, 37-24
deny lsap, 38-11
deny tcp, 37-26
deny type, 38-13
deny udp, 37-26
description
  bypass configuration mode, 22-4
  circuit configuration mode, 9-14
  dot1q PVC configuration mode, 19-2
  GRE tunnels, 24-5
  HDLC channel configuration mode, 9-14
  IMA group configuration mode, 17-29
  interface configuration mode, 7-8
  L2F configuration mode, 26-6
  L2TP configuration mode, 25-12
  port configuration mode, 9-14
dhcp max-addrs, 29-4
dhcp preserve-state, 29-6
dhcp relay option, 29-8
dhcp relay server, 29-10
dhcp relay size, 29-21
dhcp server default-lease-time, 29-14
dhcp server filename, 29-15
dhcp server max-lease-time, 29-16
dhcp server next-server, 29-17
dhcp server option, 29-18
dhcp server range, 29-20
directory, 4-15
dnis, 25-14
dns, 28-5
domain
  context configuration mode, 6-7
  L2F configuration mode, 26-8
  L2TP configuration mode, 25-16
dot1q profile, 19-3
dot1q pvc, 19-4

E

enable, 2-4
enable-peer, 34-16
encapsulation
  HDLC channel configuration mode, 12-8
  port configuration mode
    clear-channel DS-3 and E3 ports, 13-3
    Ethernet, 10-2
    HSSI, 14-2
    packet T1 and E1 ports, 15-9
  POS ports, 16-6
encapsulation-mode, 27-10
end, 2-6
equal-cost multipath routing

defined, 31-10
esp cipher, 27-12
esp hash, 27-14
ethernet encapsulation, 25-18
ethernet session, 25-19
exit, 2-7
export-non-active, 34-17

F

fabric revert, 4-17
fdl
port configuration mode
ATM T1 ports, 11-7
packet T1 ports, 15-11
T1 channel configuration mode, 12-10
format
DHCP, 29-21
system image and configuration file, 4-19
forward-time, 21-14
frame-length, 17-30
frame-relay auto-detect, 18-14
frame-relay intf-type, 18-16
frame-relay keepalive, 18-18
frame-relay lmi-n391dte, 18-20
frame-relay lmi-n392dce, 18-22
frame-relay lmi-n392dte, 18-24
frame-relay lmi-n393dce, 18-26
frame-relay lmi-n393dte, 18-28
frame-relay lmi-t392dce, 18-30
frame-relay lmi-type, 18-32
frame-relay profile, 18-34
frame-relay pvc, 18-35
frame-relay pvc default, A-1
frame-relay pvc explicit, 18-38
frame-relay pvc on-demand, 18-41
frame-relay-test, 18-44
framing
port configuration mode
ATM T1 and E1 ports, 11-9
channelized DS-3 ports, 12-11
clear-channel DS-3, 13-5
packet T1 and E1 ports, 15-12
T1 channel configuration mode, 12-11
framing sdh, 16-8
function
L2F configuration mode, 26-10
L2TP configuration mode, 25-21

G

gre-peer, 24-3
gre-tunnel, 24-10
group, 34-18

H

hardware-interface, 14-4
hash, 27-16
hdlc-channel, 12-13
header format, 43-10
hello-interval, 33-19
hello-time, 21-16
hold-time, 34-20
http server, 46-3

I

idle-cell, 11-11
ike auth, 27-17
ike group, 27-18
ike lifetime hard kbytes, 27-19
ike lifetime hard seconds, 27-21
ike lifetime soft kbytes, 27-23
ike lifetime soft seconds, 27-25
ike pre-shared-key, 27-27
ike sa_subnet, 27-28
ima enable, 17-31
ima group, 17-32
in, 27-30
interface
interfaces, 7-9
PPP, 23-9
invert-data
HDLC channel configuration mode, 12-14
port configuration mode, 15-14
ip access-group
context configuration mode
contexts, 6-9
interface configuration mode
interfaces, 7-11
IP access control lists, 37-9
ip access-list, 37-11
ip address
interface configuration mode, 7-11
subscriber configuration mode, 8-6
ip-address local, 27-31
ip-address remote, 27-32
ip arp, 8-8
ip arp arpa, 7-14
ip arp timeout, 7-15
ip bgp-community, 35-7
ip dns-ttl, 28-7
ip domain-lookup, 28-8
ip domain-name, 28-10
ip dynamic-acl timeout, 37-13
ip host
circuit configuration mode, 9-15
port configuration mode, 10-4
tunnel circuit configuration mode, 24-12

ip igmp, 36-6
ip igmp join-group
administrator exec mode, 36-8
context configuration mode, 36-8
ip igmp leave-group, 36-11
ip igmp leave-group command, 36-11
ip igmp mode, 36-14
ip ignore-df-bit, 7-16
ip irdp, 31-8
ip localhost, 28-11
ip lookup host, 7-16, 7-18
ip mask-reply, 7-20
ip maximum-paths, 31-10
ip mtu, 7-21
ip multicast max-groups, 36-15
ip multicast receive, 36-17
ip multicast-routing, 36-19
ip multicast send, 36-21
ip name-servers, 28-13
ip pool, 7-22
ip ppp-proxy-arp, 23-11
ip reflexive timeout, 37-15
ip rip interface-cost, 32-5
ip rip listen, 32-7
ip rip receive version, 32-8
ip rip send version, 32-10
ip rip split-horizon, 32-12
ip rip supply, 32-13
ip route, 31-12
ipsec key name, 27-33
ipsec lifetime hard kbytes, 27-35
ipsec lifetime hard seconds, 27-39
ipsec lifetime soft kbytes, 27-37
ipsec lifetime soft seconds, 27-41
ipsec mode, 27-43
ipsec options, 27-44
ipsec peer, 25-23
ipsec peer default, 27-45
ipsec peer name, 27-47
ipsec pfs-group, 27-48
ipsec policy name, 27-50
ipsec proposal crypto name, 27-51
ipsec proposal ike name, 27-52
ipsec tunnel policy, 27-53
ip secured-arp, 7-24
ip source-address, 7-26
ip source-validation, 8-10
ip tos-field, 8-11

K

keepalive
HDLC channel configuration mode, 12-15
port configuration mode
clear-channel DS-3 and E3 ports, 13-6
HSSI, 14-6
packet T1 and E1 ports, 15-15

L

l2f-peer name, 26-12
l2tp attribute calling-number real-circuit-id, 25-26
l2tp eth-sess-idle-timeout, 25-37
l2tp-group name, 25-24
l2tp-peer default, 25-27
l2tp-peer name, 25-29
l2tp-peer unnamed, 25-31
l2tp radius auto-group, 25-33
l2tp-tunnel domain, A-1
l2tp-tunnel name, A-1
l2x profile
L2F, 26-14
L2TP, 25-35
last-member-query-interval, 36-23
length
line configuration mode, 3-9
port configuration mode
ATM DS-3 ports, 11-13
channelized DS-3 ports, 12-16
clear-channel DS-3, 13-8
limit, 43-12
line, 3-11
linecode
ATM T1 ports, 11-14
packet T1 ports, 15-17
localdir, 43-14
local-name
L2F configuration mode, 26-16
L2TP configuration mode, 25-39
log checkpoint, 44-2
logging console, 44-3
logging filter, 44-5
logging syslog, 44-9
loopback
port configuration mode
ATM, 11-15
channelized DS-3 ports, 12-17
clear-channel DS-3, 13-9
Ethernet, 10-6
HSSI, 14-8
packet T1 and E1 ports, 15-18
POS ports, 16-9
T1 channel configuration mode, 12-17

M

mac address, 9-17
match as-path, 35-8
match community-list, 35-9

match interface, 35-10
match ip address, 35-11
match ip next-hop, 35-12
match metric, 35-13
match route-type, 35-14
match tag, 35-16
max-age, 21-17
maximum-prefix, 34-22
maximum-prefix-warn, 34-24
max-sessions
L2F configuration mode, 26-18
L2TP configuration mode, 25-41
max-tunnels
L2F configuration mode, 26-20
L2TP configuration mode, 25-43
medium, 10-7
metric, 34-26
metric-out, 34-26
minimum-links, 17-33
min-sessions, A-2
min-subscribers
L2F, 26-21
L2TP, 25-45
mkdir, 4-21
module extract, 4-23

N

neighbor, 34-28
netop server, 47-2
network, 32-14
nexthop-self, 34-29
no-aggregator-id, 34-31
nssa-sumrange, 33-21
ntp mode, 30-4
ntp server, 30-5

O

operator, 6-11
ospf-interface, 33-23
out, 27-54
outbound password, 8-13
out-delay, 34-33

P

packet-length, 16-11
passive, 34-35
password, 8-14
pbit-setting, 19-6
peer-name, 25-46
permit
bridge access control lists, 38-8
IP access control lists, 37-16
permit any, 39-3
permit context, 39-5
permit domain, 39-7
permit icmp, 37-18
permit igmp, 37-21
permit ip, 37-24
permit lsap, 38-11
permit tcp, 37-26
permit type, 38-13
permit udp, 37-26
ping, 42-24
police
GRE peer configuration mode, 24-14
L2F configuration mode, 26-22
L2TP configuration mode, 25-48
port configuration mode, 9-19
subscriber configuration mode, 8-15
port atm, 11-16
port channelized-ds3, 12-19
port ds1, 15-19
port ds3, 13-11
port e1, 15-20
port e3, 13-12
port ethernet, 10-9
port hssi, 14-10
port-limit
PPP, 23-13
subscribers, 8-16
port pos, 16-12
ports, 17-34
port te, 27-56
ppp compression, 23-15
ppp keepalive, 23-16
ppp mtu, 23-18
ppp multilink enable, 23-19
ppp multilink endpoint-discriminator, 23-21
ppp multilink mrru, 23-23
pppoe client, 23-30
pppoe motm, 23-32
pppoe services, 23-34
pppoe tag, 23-35
pppoe url
PPP, 23-37
subscribers, 8-17
ppp our-options, 23-24
ppp passive, 23-26
ppp peer-options, 23-28
precedence
BGP configuration mode, 34-37
BGP group configuration mode, 34-37
BGP peer configuration mode, 34-37
OSPF configuration mode, 33-25
RIP configuration mode, 32-16
preference
BGP group configuration mode, 34-39

BGP peer configuration mode, 34-39
priority, 21-18
privilege, 5-10
privilege max, 6-13
privilege start, 6-14
profile
L2F configuration mode, 26-24
L2TP configuration mode, 25-50
proposal crypto, 27-57
proposal ike, 27-59
protocol, 21-20

Q

query-interval, 36-25
query-response-interval, 36-27

R

radius accounting algorithm, 41-4
radius accounting deadtime, 41-6
radius accounting max-outstanding, 41-7
radius accounting max-retries, 41-9
radius accounting server, 41-11
radius accounting timeout, 41-13
radius algorithm, 41-15
radius attribute acct-session-id, 41-17
radius attribute calling-station-id, 41-19
radius attribute connect-info, 41-21
radius attribute filter-id, 41-23
radius attribute medium-type
ATM profile configuration mode, 17-36
Frame Relay profile configuration mode, 18-46
port configuration mode, 10-11
RADIUS, 41-25
radius attribute nas-ip-address, 41-27
radius attribute non-rfc-242, 41-29
radius attribute tunnel password, 41-31
radius deadtime, 41-33
radius max-outstanding, 41-35
radius max-retries, 41-37
radius server, 41-39
radius strip-domain, 41-41
radius timeout, 41-43
rate-limit
GRE peer configuration mode, 24-16
L2F configuration mode, 26-26
L2TP configuration mode, 25-52
port configuration mode, 9-20
subscriber configuration mode, 8-17
receiver, 43-16
redirect interface next-hop, 37-29
redirect interface next-hop icmp, 37-34
redirect interface next-hop ip, 37-39
redirect interface next-hop tcp, 37-44
redirect interface next-hop udp, 37-44
redistribute
BGP configuration mode, 34-41
OSPF configuration mode, 33-27
RIP configuration mode, 32-18
reflexive ftp, 37-50
reflexive tcp, 37-53
reflexive tftp, 37-50
reflexive udp, 37-53
reload, 4-25
remotefile, 43-18
remove-private-AS, 34-43
rename, 4-27
retransmit-interval, 33-29
retry
L2F configuration mode, 26-28
L2TP configuration mode, 25-54
rmdir, 4-29
rmon alarm, 45-4
rmon event, 45-6
robustness, 36-29
route-access-list
extended-access-list-number, 35-17
standard-access-list-number, 35-19
route-map
BGP peer configuration mode, 34-45
context configuration mode, 35-21
router bgp, 34-47
routerdead-interval, 33-30
route-reflector-client, 34-50
router-id
BGP, 34-49
OSPF, 33-32
router-igmp-interface, 36-31
router igmp-proxy, 36-33
router ospf, 33-33
router-priority, 33-34
router rip, 32-20

S

sample-interval, 43-20
save configuration, 4-31
save log, 44-11
schema, 43-21
schema-dump, 43-24
schema profile, 43-25
scramble
ATM ports, 11-17
POS ports, 16-13
secondary-tunnel-auth, 25-56
service access-list, 39-9
session-auth
L2F configuration mode, 26-30

L2TP configuration mode, 25-58
set as-path prepend, 35-23
set community, 35-25
set ip next-hop, 35-27
set local-preference, 35-29
set metric, 35-30
set origin, 35-32
set preference, 35-33
shaping, 17-38
show administrator reservations, 3-12
show administrators, 42-26
show as-path-access-list, 35-34
show atm counters, 17-40
show atm multicast, 17-43
show atm profile, 17-47
show atm pvc, 17-49
show atm range, A-2
show atm vp, 17-52
show bert
channelized DS-3 ports, 12-20
packet T1 and E1 ports, 15-21
show bindings, 20-22
show bridge access-list, 38-15
show bridge address, 21-22
show bridge info, 21-23
show bridge span-tree, 21-24
show bridge table, 21-27
show bulkstats, 43-28
show bypass, 22-5
show clock, 5-12
show cm stats, 42-28
show cm table, 42-33
show community-list, 35-35
show configuration, 4-33
show context, 6-15
show debugging, 42-35
show dhcp, 29-23
show dhcp server lease, 29-26
show dhcp server sram, 29-28
show diag, 42-37
show dot1q counters, 19-7
show dot1q profile, 19-9
show dot1q pvc, 19-10
show envmon, 42-41
show fabric counters, 42-42
show fabric table, 42-44
show fe stats, 42-47
show frame-relay counters, 18-48
show frame-relay lmi-config, 18-51
show frame-relay lmi-errors, 18-53
show frame-relay lmi-stats, 18-55
show frame-relay multicast, 18-57
show frame-relay profile, 18-60
show frame-relay pvc, 18-62
show frame-relay range, A-2
show gre counters, 24-18
show gre info, 24-20
show gre tunnel counters, 24-22
show gre tunnel info, 24-23
show hardware, 42-52
show hdlc-channel counters, 12-21
show hdlc-config, 12-23
show ima group, 17-52
show ima pmon, 17-54
show ip access-list, 37-57
show ip arp
interfaces, 7-27
subscribers, 8-18
show ip bgp, 34-52
show ip bgp groups, 34-55
show ip bgp neighbors, 34-57
show ip bgp paths, 34-60
show ip bgp summary, 34-62
show ip dynamic-acl subscriber, 37-59
show ip host, 6-17
show ip igmp, 36-34
show ip interface, 7-29
show ip localhosts, 28-15
show ip ospf, 33-35
show ip ospf area, 33-37
show ip ospf border-router, 33-39
show ip ospf database, 33-41
show ip ospf interface, 33-45
show ip ospf neighbor, 33-47
show ip ospf summary-range, 33-49
show ip pool, 7-32
show ip ppp-proxy-arp
configuring interfaces, 7-33
configuring PPP, 23-39
show ip reflexive-acl, 37-61
show ip route, 31-16
show ipsec peer, 27-60
show ipsec stats, 27-62
show ip secured-arp, 7-33
show ip socket, 42-56
show ip static-route, 31-19
show ip traffic
contexts, 6-19
system monitoring, 42-57
show l2f counters, 26-32
show l2f info, 26-35
show l2tp counters, 25-60
show l2tp group, 25-67
show l2tp info, 25-69
show log, 44-13
show logging, 44-17
show memory, 42-59
show ntp associations, 30-7

show ntp status, 30-9
show pmon
channelized DS-3 ports, 12-25
packet T1 and E1 ports, 15-22
show port counters, 9-21
show port diag, 9-29
show port info, 9-33
show port table, 9-35
show ppp, 23-41
show ppp compression, 23-44
show ppp multilink, 23-46
show pppoe, 23-48
show pppoe counters, 23-50
show pppoe services, 23-52
show privilege
contexts, 6-21
user interface, 2-8
show process, 42-61
show radius counters, 41-45
show route-access-list, 35-36
show route-map, 35-37
show service access-list, 39-11
show slot, 42-63
show snmp, 45-8
show snmp server, 45-10
show sram, 42-64
show stack, 42-66
show subscribers
subscribers, 8-20
system monitoring, 42-67
show t1 info
channelized DS-3 ports, 12-28
packet T1 ports, 15-24
show tech, 42-70
show te cpu, 27-65
show te performance, 27-67
show te ps, 27-68
show terminal, 3-13
show te time, 27-70
show username-format, 40-37
show version, 4-35
shutdown
HDLC channel configuration mode, 9-37
port configuration mode, 9-37
slowsync, 30-11
snmp community, 45-12
snmp engine-id, 45-14
snmp group, 45-16
snmp manager, A-2
snmp notify, 45-18
snmp notify-filter, 45-20
snmp notify-target, 45-22
snmp server, 45-24
snmp set, 45-26
snmp target, 45-26
snmp target-parameters, 45-29
snmp user, 45-31
snmp view, 45-33
speed
HDLC channel configuration mode, 12-30
port configuration mode, 15-26
spf-timers, 33-52
spi in, 27-71
spi out, 27-72
sshd keygen, 3-14
startup-query-interval, 36-40
static, 25-77
subscriber, 8-23
symmetry, 17-57
system contact, 5-13
system hostname, 5-14
system location, 5-15

T

t1, 12-31
telnet, 3-15
terminal length, 3-17
terminal monitor, 3-18
terminal width, 3-20
throttle, 34-64
timeout
administrator configuration mode, 6-22
L2F configuration mode, 26-37
L2TP configuration mode, 25-79
subscriber configuration mode, 8-25
timeslot, 15-27
transfer-interval, 43-30
transmit-delay, 33-54
ts16, 15-29
ttl, 34-65
tunnel-auth
L2F configuration mode, 26-39
L2TP configuration mode, 25-81
tunnel domain
L2F, 26-41
L2TP, 25-83
tunnel ip, 27-73
tunnel map, 24-25
tunnel name
L2F, 26-43
L2TP, 25-85
tunnel-window, 25-86

U

unsolicited-report-interval, 36-42

V

version, 32-21
version1-router-interval, 36-44

W

width, 3-21

Y

yellow-alarm
    port configuration mode
        ATM T1 and E1 ports, 11-18
        packet T1 and E1 ports, 15-30
    T1 channel configuration mode, 12-32